Conférence d'Alain Connes "*Évariste Galois et la théorie de l'ambiguïté*", à l'Académie des Sciences, dans le cadre du Colloque pour le bicentenaire de la naissance de Galois (29 novembre 2011).

Le Président de séance : Bien, mesdames, messieurs, nous avons à l'évidence une séance exceptionnelle, d'ailleurs, une audience exceptionnelle, mais pour un homme exceptionnel, dont la vie, exceptionnellement courte, a été exceptionnellement productive. Nous avons la chance d'avoir Alain Connes, qui va nous parler d'un aspect particulier d'Évariste Galois, qui est la relation que Galois a entretenue avec les académiciens des sciences à l'époque. Alain Connes, vous avez la parole.

Alain Connes : En fait, mon exposé aura deux parties. Dans la première partie, j'expliquerai, si vous voulez, effectivement les relations très complexes, beaucoup plus complexes qu'on ne le dit, entre Évariste Galois et les académiciens de son époque. Et dans la deuxième partie, j'essaierai de vous expliquer, de la manière la plus simple possible, ce qu'est la théorie de l'ambiguïté.

Donc, je commencerai par vous montrer un portrait bien connu d'Évariste Galois. Et ensuite, on ira très, très rapidement à travers une chronologie que je n'utiliserai que quand j'en aurai besoin, parce que, si vous voulez, je vous décrirai en gros ce qui s'est passé pendant ces trois années, qui marquent la fin de la vie de Galois. Et donc, je ne reviendrai dans les détails de la chronologie qu'occasionnellement.

Et donc, vous m'excuserez si je passe très vite sur cette chronologie. Après, on reprendra le fil des événements de manière beaucoup plus lente. Donc, la chronologie, évidemment, Galois naît il y a 200 ans, le 25 octobre 1811.

La première date marquante, c'est en avril 1829, c'est la mort d'Abel, parce qu'on verra que les destins d'Abel et de Galois sont incroyablement reliés l'un à l'autre. À la même époque, le 25 mai et le 1er juin, Cauchy présente les premiers travaux de Galois à l'Académie. Cette même année, en juillet, le père de Galois se suicide.

Galois échoue pour la deuxième fois à Polytechnique, mais il est reçu à l'ENS, ce qui s'appelait à l'époque l'École préparatoire. Le 18 janvier 1830, il y a une lettre de Cauchy très importante que je vous montrerai. Et en février 1830, Cauchy remet au Secrétaire perpétuel de l'Institut, qui était Joseph Fourier, le mémoire de Galois sur les conditions de résolubilité des équations par radicaux.

Et il lui demande, justement, de faire concourir ce Mémoire pour le Grand Prix des Sciences mathématiques. Le 28 juillet 1830, le Grand Prix des sciences mathématiques de l'Académie est attribué à Abel et Jacobi. La même année, en juillet, c'est un événement politique très important, les Trois Glorieuses, que vous connaissez tous, mais qui fait que Cauchy part.

Donc Cauchy part de France pour de nombreuses années. Il va à Turin. En janvier 1831, Galois est exclu de l'École Normale.

Le 13 janvier 1831, il inaugure, dans une librairie au 5 rue de la Sorbonne, on y reviendra, avec 30 élèves, un cours privé d'Algèbre supérieure, visant explicitement à suppléer les carences de l'enseignement public. La même année, en 1831, Galois réécrit et soumet à l'Académie, sur les conseils de Poisson (Poisson faisait partie du jury qui a exclu Galois de l'École Normale), son mémoire perdu relatif aux conditions de résolubilité des équations algébriques par radicaux. Le 9 mai, il est arrêté. Il y a un banquet bien connu, qui était donné pour l'acquittement de certains républicains, et Galois avait levé son verre à Louis-Philippe, mais en tenant un couteau à la main. Le 15 juin, il est acquitté. Le 4 juillet 1831, il reçoit le rapport négatif de Poisson sur ses travaux. On le verra, ce rapport, je l'ai dans les documents. Et bon, ensuite, la fin, vous la connaissez, Galois passe de nombreux mois en prison. Il est arrêté le 14 juillet, peu de temps après avoir reçu le rapport de Poisson, il est arrêté à la tête d'une manifestation. Et cette fois, il est arrêté pour port d'arme illégal. Il n'est pas jugé par un jury (il y avait un jury populaire), donc, il reste en prison très, très longtemps. Il est enfermé à la prison Sainte-Pélagie. Il en ressort le 16 mars, mais simplement parce qu'il y a le choléra dans Paris.

Et il est libéré, mais pas vraiment : il est dans une maison de santé privée. Et enfin, bon, il y a le mercredi 30 mai qui est le jour du duel et il meurt le lendemain.

Alors, évidemment, ça, c'est extrêmement rapide, c'est simplement pour vous donner quelques repères. Et on y reviendra quand on aura des problèmes de date. Donc, un personnage central, c'est le personnage d'Abel qui meurt le 5 avril 1829, alors que Galois a 17 ans.

Et Abel avait eu déjà des relations assez complexes et assez compliquées avec Cauchy. Et je vais vous montrer une lettre d'Abel dans laquelle il parle de Cauchy. Je m'inspire là, bien sûr, d'un merveilleux article d'*Histoire des mathématiques* de René Taton, sur lequel je reviendrai à maintes reprises.

Donc, Abel écrit à propos d'Augustin Cauchy la chose suivante :

> *"Cauchy est fou et il est impossible d'avoir affaire avec lui. Pourtant, c'est lui qui, à présent, est le mathématicien qui sait comment doivent être traitées les mathématiques. Ses travaux sont excellents, mais il écrit obscurément.*
>
> *D'abord, je ne comprenais presque rien à ses œuvres. Maintenant, j'y arrive mieux. Cauchy est infiniment catholique et bigot. Chose bien singulière pour un mathématicien ! D'ailleurs, il est le seul qui travaille les mathématiques pures. Poisson, Fourier, Ampère, etc. s'occupaient exclusivement de magnétisme et d'autres parties de la physique."*

Donc ça, c'est une lettre qu'Abel avait écrite en 1826. Il est bien connu que Cauchy et l'Académie ont pris du temps pour reconnaître les travaux d'Abel, mais ça a été fait.

Donc ça, c'est un portrait de Galois qui a été fait, je pense, par Augustin Chevalier, de mémoire, après la disparition de Galois. Mais qui dit beaucoup de choses sur Galois, en fait. Donc la relation entre Galois et Abel est très intéressante.

Alors voilà ce que Galois a écrit. En gros, si vous voulez, ce qui s'est passé, c'est que Galois, en 1829, avait donné deux manuscrits à l'Académie. Et après la mort d'Abel, il a appris que ses travaux étaient largement anticipés par ceux d'Abel.

Et ça lui a donné un coup, évidemment. Mais bon, voilà ce qu'il dit après[1].

> *"Dans tous les cas, il me serait aisé de prouver que j'ignorais même le nom d'Abel quand j'ai présenté à l'Institut, mes premières recherches sur la théorie des équations, et que la solution d'Abel n'aurait pu paraître avant la mienne.*

Donc ça, c'est écrit à la prison, quand il était à la prison Sainte-Pélagie, en décembre 1831, donc la dernière année de sa vie. Cette note a pour but essentiel d'affirmer l'indépendance des travaux de Galois par rapport à ceux d'Abel. Galois qui connaissait alors une lettre qu'Abel avait envoyée à Legendre, il y avait une très longue correspondance entre Abel et Legendre, le 25 novembre 1828. Et voilà ce que dit Galois. Il dit :

> *"Mais la mort anticipée de ce géomètre, ayant privé la science des recherches promises dans cette lettre, il n'en était pas moins nécessaire de donner la solution d'un problème qu'il m'est bien pénible de posséder, puisque je dois cette possession à une des plus grandes pertes qu'aura faite la science."*

Donc il n'y avait pas du tout d'antipathie ou quoi que ce soit, il n'y avait même pas de rivalité. En gros, si vous voulez, Abel disparaît exactement où Galois commence à exister dans le paysage mathématique. Donc voilà Cauchy.

Il est né en 1789, donc quand Galois naît, il avait déjà 22 ans. Je veux dire, c'était un mathématicien extraordinaire. Et la relation entre Galois et Cauchy est extrêmement intéressante. Comme je vous l'ai dit, Cauchy est parti de France en 1830. Et à ce moment-là, il n'a plus eu de contact avec Galois. Donc les meilleurs renseignements que l'on ait sur les relations entre Cauchy et Galois, qui bien souvent sont présentées de manière complètement caricaturale, c'est à travers un article de René Taton, un grand historien des mathématiques, qui est mort en 2004, et qui nous dit la chose suivante.

Il nous dit :

> *"Parmi les très rares renseignements qu'elles nous apportent à ce sujet, les archives de l'Académie des sciences révèlent que Galois eut le privilège de voir ses premiers travaux [a] présentés devant l'Académie au cours des séances des 25 mai et 1^er^ juin 1829 [b] par un juge aussi sévère que compétent, Cauchy. Bien qu'aucune précision ne nous soit parvenue sur ce point, l'acceptation par le grand analyste de cette tâche de présentation prouve que le jeune auteur de ces mémoires avait réussi à le convaincre du sérieux, de l'importance et de l'originalité de ses recherches."*
>
> [a] Galois avait 17 ans.
> [b] En mai-juin 1829, Galois avait 17 ans puisqu'il est né en octobre.

[1] en 1829.

Alors, un peu après, pendant le début de l'été 1829, le mémoire d'Abel sur les équations algébriques est paru de manière posthume et bien sûr, Cauchy a constaté qu'une bonne partie des résultats obtenus par Galois étaient absorbés par le mémoire d'Abel.

Donc, il était de son devoir d'essayer d'atténuer la déception de Galois, en l'encourageant à sauver la part la plus originale de son travail. On verra qu'il y avait une part extrêmement originale, même à cette époque-là.

> "*Lorsqu'il se décida au début de 1830 à rédiger son rapport sur les mémoires de Galois, on peut penser que dans cette circonstance, Cauchy songea beaucoup moins à remplir une obligation académique qu'à apporter d'utiles conseils au jeune mathématicien. Toujours est-il que ce rapport fut rédigé pour être lu à la séance de l'Académie du 18 janvier 1830 et que seule une indisposition empêcha Cauchy de le présenter.*"

Alors, j'espère qu'on va voir la lettre. J'ai écrit le texte en clair.

C'est une lettre d'excuse :

> "*Monsieur le Président,*
>
> *Je me proposais de présenter aujourd'hui à l'Académie le rapport sur les travaux du jeune Galois, un mémoire sur la détermination analytique des racines primitives dans lequel on fait voir comment on peut réduire cette détermination à la résolution d'équations numériques, etc.*
>
> *Retenu chez moi par une indisposition, je regrette de ne pouvoir assister à la séance de ce jour et je vous prie de bien vouloir inscrire mon nom sur l'ordre du jour de la séance suivante. Agréez, je vous prie, l'hommage...*"

Donc, c'est une lettre de Cauchy qu'on retrouve dans les archives de l'Académie et qui montre que, bien sûr, Cauchy n'ignorait absolument pas Galois, il y avait des relations très, très fortes entre Cauchy et Galois à cette époque-là. Il y a cette lettre. Et en fait, voilà ce que dit René Taton.

Il dit :

> "*Du fait du report annoncé de ce rapport, donc le rapport de Cauchy sur Galois à la séance suivante, celle du 25 janvier 1830, nous* (c'est René Taton) *avons examiné avec un soin tout particulier les différentes pièces concernant cette séance : dossier, primitif, registre de procès-verbaux. Mais alors que ces divers documents montrent que Cauchy, effectivement présent, y présenta bien son mémoire annoncé* "Sur la détermination des racines primitives dans la théorie des nombres", *rien n'y rappelle le premier point évoqué dans sa lettre du 18 janvier, le* "*Rapport sur les travaux du jeune Galois*".

L'étude des procès-verbaux des séances de l'Académie révèle que, non seulement ce rapport annoncé par écrit pour la séance du 25 janvier, n'y a pas été présenté, mais qu'aucune allusion n'y a plus été faite au cours des séances suivantes. Le fait que Galois ne se soit jamais plaint de la négligence de Cauchy en cette circonstance, alors qu'il plaçait tous ses espoirs en un jugement favorable de l'Académie, semble montrer que l'annulation de ce rapport est intervenue avec son accord. Il reste alors à expliquer ce brusque changement d'attitude des deux acteurs de cette mystérieuse affaire."

La thèse de René Taton, et je pense que c'est quelque chose qui est parfaitement plausible, est :

"*La confrontation attentive des quelques éléments d'information permet de formuler à ce sujet une hypothèse qui paraît vraisemblable.*"

Son hypothèse, c'est que Cauchy avait demandé à Galois de réécrire son manuscrit, de manière plus détaillée, de telle sorte qu'il soit présenté au Grand Prix de l'Académie. Quel Grand Prix de l'Académie ? Il y avait un concours. En fait, ce n'était pas un Grand Prix, c'était un concours. Ça s'appelait un concours à l'époque.

C'était un concours qui était formulé de la manière suivante.

"*Le prix sera décerné à celui des ouvrages, ou manuscrits, ou imprimés, qui présentera l'application la plus importante des théories mathématiques, soit à la physique générale, soit à l'astronomie, ou qui contiendra une découverte analytique très remarquable.*".

Donc, ce Grand Prix se distinguait également par le fait que les travaux publiés entre le 1^er^ janvier 1828 et le 1^er^ janvier 1830, séparément ou dans des recueils scientifiques, pouvaient être pris en considération par le jury sans que leur auteur ait fait acte de candidature, concurrentement avec les ouvrages ou mémoires qui étaient déposés au secrétariat de l'Institut avant le 1^er^ mars 1830.

Donc, en fait, ce Grand Prix a permis à l'Académie de réparer l'injustice qui avait été faite à Abel dans les années précédentes, la lenteur du processus de jugement des écrits d'Abel, le fait qu'ils avaient été reconnus de manière tardive. Et en fait, donc, le Grand Prix a été attribué à Abel conjointement à Jacobi. Et c'était évidemment parfaitement mérité : si on regarde la liste des candidats, c'est une liste époustouflante. Donc, ce que pense René Taton : il pense, comme je vous l'ai dit, que Cauchy persuada Galois de rédiger son mémoire pour le Grand Prix de mathématiques, un mémoire de synthèse qui réunissait l'ensemble de ses contributions, en même temps que les mémoires de 1829. Donc, évidemment, les espoirs que Galois plaçait dans le concours du Grand Prix de l'Académie devaient se trouver cruellement déçus.

Il ne pouvait pas raisonnablement ressentir comme une injustice, bien sûr, le fait que le 28 juin, le prix ait été accordé à Abel et à Jacobi. Mais par contre, là où il a commencé à devenir un peu paranoïaque, on peut dire, c'est qu'il a appris à ce moment-là que son manuscrit avait été perdu. Alors, la raison est complexe.

La raison est que Cauchy ne faisait pas partie des examinateurs, pour le Grand Prix, il n'en faisait pas partie. Le secrétaire perpétuel, c'était Joseph Fourier.

Et Joseph Fourier est mort en mai de cette année-là. Donc, il a disparu avant même que le Grand Prix ait été attribué. Et, en fait, les recherches montrent que, bien sûr, l'explication qui a été donnée à Galois ne tenait pas. On lit :

> *"C'est une chose bien simple", aurait repondu Cuvier à une réclamation de Galois..."*

Le mémoire a été perdu à la mort de Fourier, qui était chargé de l'examiner. Donc, c'était effectivement Fourier qui était chargé de présenter les travaux de Galois pour le Grand Prix. Ce n'était pas Cauchy.

> *"...et l'on conçoit, bien sûr, que ce nouveau malheur,..."*

(le fait que son manuscrit ait été perdu, à l'époque, il n'y avait pas beaucoup de photocopieuses !, donc, le fait que son manuscrit ait été perdu),

> *"...ait été vécu par lui comme presque une attaque personnelle."*

Et en fait, les recherches montrent qu'il a été perdu par le Secrétariat de l'académie. Donc, Galois l'a pris comme étant une injustice terrible.

Et voilà ce que dit Galois. Voilà ce qu'il dit dans ses écrits.

> *"Il suffira de dire que mon mémoire sur la théorie des équations a été déposé en substance à l'Académie des sciences en février 183...0"*

(c'était l'année du concours, c'était l'année où Cauchy lui avait demandé de déposer son mémoire),

> *"...que des extraits en avaient été envoyés en 1829..."*

(donc, ce sont les deux articles qu'il avait déposés au printemps de 1829, quand il avait 17 ans).

> *"...qu'aucun rapport ne s'en est suivi et qu'il m'a été impossible de revoir les manuscrits."*

Donc, il lui a été impossible de revoir les manuscrits, effectivement, parce qu'ils ont été perdus à la mort de Fourier. Il devait y avoir un désordre dans tous les papiers. Et son manuscrit a été perdu.

Alors, voilà ce que dit Auguste Chevalier, qui était un ami très, très proche de Galois, auquel Galois se confiait. Voilà ce qu'il dit à ce moment-là :

> *"Le peu d'attention donnée par l'Institut au premier travail soumis à son jugement par Galois commença pour lui des douleurs qui, jusqu'à sa mort, devaient se succéder de plus en plus vives."*

Donc, il avait un sentiment d'injustice.

> *"Une telle indifférence aurait suffi pour guérir de toute ardeur scientifique. Mais il n'en fut point abattu. Une puissante nature le poussait en avant."*

Alors, le deuxième épisode, c'est donc à ce moment-là, en 1830. Donc, il y a les Trois Glorieuses. Galois est enfermé à l'École Normale. On ne laisse pas les élèves de l'École Normale, enfin, de l'École Préparatoire, sortir, alors qu'on laisse sortir ceux de l'École Polytechnique. Enfin, on ne les laisse pas sortir, mais ils font le mur. Ils vont sur les barricades.

Et à partir de ce moment-là, Galois éprouve une aversion pour le Directeur de l'École Normale de l'époque. Et il fait tant et si bien que finalement, il finit par se faire renvoyer de l'École Normale. Alors, donc, il est renvoyé de l'École Normale fin décembre, début janvier de 1831, de l'année suivante.

Et la personne, d'abord, qui signe l'arrêt de renvoi de Galois de l'École Normale, c'est un certain Victor Cousin. Et la rue Victor Cousin est la rue dans laquelle Galois a donné ses cours après avoir été renvoyé de l'École Normale. Il a donné son cours d'algèbre, avec 35 élèves.

Il n'y a pas dans Paris de rue Galois. Il y en a une qui est en dehors du périphérique. Et je pense que ce serait une bonne idée qu'au moins, qu'on ne change pas le nom de la rue, ce n'est pas la peine, mais qu'il y ait une plaque dans la rue de la Sorbonne, la rue Victor Cousin, qui explique clairement que Galois a donné ses cours à cet endroit-là après s'être fait renvoyer de l'École Normale.

Alors, le rapport avec Poisson est très intéressant parce que Poisson, qui faisait partie du comité (ce n'était pas un jury) qui a renvoyé Galois de l'École Normale, a sûrement parlé à Galois en privé, et lui a dit qu'il fallait qu'il redonne son manuscrit pour qu'il soit examiné par l'Académie. Je vous rappelle que Cauchy n'était plus présent. Cauchy était à Turin, donc Galois n'avait plus de protecteur direct. Il n'avait pas de personne à laquelle il pouvait s'adresser à l'Académie.

Et je pense qu'il a parlé à Poisson. Et donc, à ce moment-là, il a donné à Poisson son manuscrit. Et voilà, je vais vous lire le rapport. C'est un rapport de référé qui a été lu à la séance du 11 juillet 1831, cette même année, donc peut-être quelques six mois après, et qui est le rapport que Poisson et Lacroix ont rédigé sur le Mémoire de Galois.

Donc, ce rapport est extrêmement bien fait. Je veux dire, ce n'est pas du tout une négligence. C'est un rapport qui est extrêmement précis et bien argumenté.

Donc, voilà ce que dit Poisson :

"*L'auteur entend par équation irréductible une équation dont les coefficients sont rationnels* (donc on en verra des dizaines), *et qui ne peut se décomposer en d'autres équations, qui aient aussi leurs coefficients rationnels*" (parce que si vous avez une équation qui s'écrit comme produit, le polynôme s'écrit comme produit de plusieurs polynômes, il suffit de regarder chacun des polynômes).

"D'après sa proposition, l'équation générale..."

Alors, quelle est la proposition de Galois ? Il dit que

"pour qu'une équation irréductible de degré premier soit soluble par radicaux, il faut et il suffit que deux quelconques de ses racines étant connues, les autres s'en déduisent rationnellement".

Alors, pour les mathématiciens, ça, ça veut dire que l'extension galoisienne correspondante est engendrée par deux quelconques des racines, distinctes, de l'équation. On verra ce que ça signifie au niveau théorie des groupes.

Donc, c'est ça le critère que Galois entendait prouver pour les équations de degré premier.

"Alors, donc, l'auteur entend par équation irréductible, on l'a vu. D'après sa proposition..."

Donc, ce qu'il propose, évidemment, si vous prenez une équation de degré 3, 3 est premier, et si vous connaissez deux racines, vous connaissez la troisième, puisque vous avez, par exemple, la somme ou le produit qui est connu. Donc, ça, c'est une remarque triviale. Maintenant, on vient à un point plus embêtant.

Donc, il dit :

"Des notes trouvées dans les papiers d'Abel, qui ont été imprimées après sa mort dans le journal de Crelle, tome V, page 345, renferment une proposition analogue à celle de M. Galois, dont voici l'énoncé. Si trois racines d'une équation quelconque irréductible, dont le degré est un nombre premier, sont liées entre elles de sorte que l'une de ces racines puisse être exprimée rationnellement au moyen des deux autres, l'équation dont il s'agit sera toujours résoluble à l'aide de radicaux".

Alors, cet énoncé diffère de celui de Galois en ce que le géomètre norvégien ne dit pas que la condition dont il s'agit soit nécessaire, mais seulement qu'elle suffit pour que l'équation soit résoluble.

"Et il ne semble pas qu'il la regardât comme indispensable, car on trouve dans les notes citées une autre proposition relative à la résolution d'une classe nombreuse d'équations qui pourraient bien ne pas remplir cette condition. Il ne paraît pas non plus que ce soit à cette proposition qu'il ait fait allusion dans ce passage d'une lettre écrite à M. Legendre et publiée après la mort d'Abel dans le journal de Crelle, dans laquelle il dit", ça c'est Abel qui parle, *"J'ai été assez heureux, dit-il, de trouver une règle sûre à l'aide de laquelle on pourra reconnaître si une équation quelconque proposée est résoluble ou non à l'aide de radicaux. Un corollaire de ma théorie fait voir que généralement il est impossible de résoudre des équations supérieures au quatrième degré."*

"Alors nous ignorons si Abel a laissé un manuscrit de cette théorie, elle n'a point encore été imprimée, non plus que la démonstration du théorème analogue à celui qui fait l'objet de ce rapport et qui appartiendrait entièrement à Galois, s'il parvenait à l'établir d'une manière satisfaisante. Toutefois, on doit remarquer qu'il ne renferme pas, comme le titre du Mémoire le promettait, la condition de résolubilité des équations par radicaux. Car, en admettant comme vraie la proposition de Galois, on n'en serait guère plus avancé pour savoir si une équation donnée, dont le degré est un nombre premier, est résoluble ou non par des radicaux".

"Puisqu'il faudrait d'abord s'assurer si cette équation est irréductible". Ça, c'est vraiment du pinaillage, parce que s'assurer d'abord si l'équation est irréductible, ce n'est pas très difficile. *"Et ensuite, si l'une de ses racines peut s'exprimer en fonction rationnelle des deux autres".*

Ça, c'est beaucoup plus difficile.

"La condition de résolubilité, si elle existe (alors là Poisson est vraiment très terre à terre), il dit, *devrait être un caractère extérieur que l'on pût vérifier à l'inspection des coefficients d'une équation donnée, ou, tout au plus, en résolvant d'autres équations d'un degré moins élevé que celui de la proposée.".*

On verra qu'il y a toute une histoire ultérieure derrière ça qui est très très intéressante. *"Quoi qu'il en soit, nous avons fait tous nos efforts pour comprendre la démonstration de Galois. Ses raisonnements ne sont ni assez clairs, ni assez développés pour que nous ayons pu juger de leur exactitude et nous ne serions pas en état d'en donner une idée dans son rapport".*

"L'auteur annonce que la proposition qui fait l'objet spécial de son Mémoire est une partie d'une théorie générale susceptible de beaucoup d'autres applications. Souvent, il arrive que les différentes parties d'une théorie, en s'éclairant mutuellement, sont plus faciles à saisir dans leur ensemble qu'isolément. On peut donc attendre que l'auteur ait publié en entier son travail pour se former une opinion définitive mais dans l'état où est maintenant la partie qu'il a soumise à l'Académie, nous ne ne pouvons pas vous proposer d'y donner votre approbation".

Alors, je vais simplement vous raconter une anecdote. C'est que quand Galois a reçu ce rapport, c'était le 4 juillet 1831, il a écrit en dessous "Ô Chérubins !". Parce que... Pardon, ce qu'il a écrit en dessous de ce rapport quand il a eu le rapport de Poisson le 4 juillet, il a écrit en dessous "Ô Chérubins". C'est-à-dire, vous n'avez pas bien compris, c'est-à-dire il faut bien admettre que la manière dont Galois a écrit est extrêmement elliptique. Mais, on verra aussi en lisant un peu en détail à quel point il va exactement au point le plus profond.

Donc, ce qui est vrai, c'est que, par exemple, si on lit ce que Galois a écrit pour démontrer ce théorème qu'une équation de degré premier est résoluble par radicaux, si et seulement si toute racine est fonction rationnelle des deux autres, c'est très difficile à comprendre. Par contre, il avait la démonstration de manière complète, ça c'est clair. En fait, ce qui est très amusant aussi, c'est que pour démontrer ce théorème, il faut utiliser un résultat de Cauchy que Galois utilise, qui est que si on prend un groupe fini dont l'ordre est divisible par un nombre premier qui agit sur un ensemble à p éléments, il contient une permutation cyclique d'ordre p. En fait, il connaissait aussi la théorie de Sylow.

Si on regarde ses papiers, il connaissait aussi le fait que ça contient un groupe d'ordre p^n, où p^n est la plus grande puissance qui permet de diviser l'ordre du groupe. Alors en fait, donc, la situation était très mauvaise à ce moment-là. Comme je l'ai dit, quelques jours après avoir reçu le rapport de Poisson, Galois devait être vraiment découragé dans un état assez instable, et c'est à ce moment-là qu'il a été arrêté à la tête de la manifestation et qu'il s'est retrouvé à la prison pour pratiquement le reste de sa vie.

Donc les choses auraient pu en rester là, et puis il y a un miracle, et ce miracle c'est Joseph Liouville, qui est aussi un membre de l'Académie, et qui est un contemporain de Galois, ça il faut le savoir, c'est-à-dire Galois est né en 1811, vous voyez, Liouville est né en 1809, donc il est exactement de la même génération que Galois. Et la résurrection de Galois, de ses Œuvres, on peut le dire, ce serait trop facile de dire que, je veux dire que ça aurait été trouvé de toute manière, parce qu'il s'est écoulé plus de dix ans entre la disparition de Galois et le moment où Liouville a étudié de manière extrêmement soigneuse et précautionneuse les papiers qui lui avaient été remis par le frère de Galois et par Auguste Chevalier, qui était la liasse de papier que Galois a laissé la veille de sa mort.

Et voilà ce que dit Liouville dans la séance du 4 septembre 1843. Donc c'est plus de dix ans après. Donc c'est un peu écrit en petit, mais je l'ai écrit en clair, mais je voulais simplement vous montrer comment ça apparaît dans les registres de l'Académie.

Donc ce que dit Liouville, c'est :

"À la suite d'une discussion où l'on a tant parlé d'équations algébriques, j'espère intéresser l'Académie en lui annonçant que dans les papiers d'Évariste Galois, donc ces manuscrits m'ont été confiés par Auguste Chevalier, j'ai trouvé une solution aussi exacte que profonde de ce beau problème : "étant donné une équation irréductible de degré premier, décider si elle est ou non résoluble à l'aide de radicaux". "Le mémoire de Galois est rédigé peut-être d'une manière un peu trop concise (ça c'est évident), je me propose de le compléter, donc il a fait le travail, de le compléter par un commentaire qui ne laissera, je crois, aucun doute sur la réalité de la belle découverte de notre ingénieux et infortuné compatriote."

Donc ça c'est merveilleux, c'est merveilleux, parce qu'en fait il a fallu attendre deux ans après cette séance de l'Académie, du 4 septembre 1843, pour que les papiers de Galois soient publiés par Liouville, dans ce qui s'appelle maintenant, je pense, le Journal de Liouville.

Et à ce moment-là, il faut dire, ils ont eu une influence absolument considérable. Bon, alors voilà pour la partie historique, voilà pour la partie historique, voilà pour la partie qui concerne ces relations entre Galois et l'Académie, mais vous voyez à quel point ces relations sont complexes. Ce sont des relations extrêmement complexes, et on aurait tort de les caricaturer en disant que Galois haïssait, c'est vrai qu'il a écrit des choses un peu exagérées, mais il s'est retrouvé dans une situation dans laquelle il était devenu presque paranoïaque.

Alors maintenant, donc, je vais vous parler de mathématiques, je vais essayer de vous expliquer ce qu'est la théorie de l'ambiguïté, mais comme la voyait Galois. Alors, vous voyez, d'abord, quand vous parlez de théorie de l'ambiguïté, ça paraît absolument absurde, parce que si je vous donne une équation, j'ai pris une équation simple, ici, là, une équation de degré 5, je me contenterai du degré 5, à la fois parce qu'il est premier, et puis parce qu'on peut faire toutes sortes de choses. Donc si vous prenez une équation, et si je vous dis il y a une ambiguïté entre les racines, vous pouvez me rire au nez, puisque les racines, j'ai pris l'équation pour que les racines soient réelles, il y en a une qui est la plus petite, c'est A, et puis comme ça, elles sont en ordre croissant.

Donc vous voyez bien qu'il n'y a pas d'ambiguïté entre les racines, elles sont toutes devant vous. Mais maintenant, supposez que je vous demande, je vous pose une question, je vous dis, est-il possible de nommer la plus grande racine, par exemple E, par une relation qui ne laissera pas, justement, d'ambiguïté sur le fait que c'est la plus grande racine, et qui soit une relation rationnelle. Alors j'ai écrit cette relation $E = 4C^2 + 2D^2$, parce que quand vous faites les calculs avec l'ordinateur, vous avez l'impression qu'elle est vraie.

Alors pourquoi est-ce que cette relation ne peut pas être vraie ? La théorie de Galois a cette force, si vous voulez, que c'est une théorie qui vous permet de savoir, à partir de rien, simplement par un raisonnement abstrait, et ça va aller beaucoup plus loin après, dans des circonstances beaucoup plus générales, pour qu'on sache qu'une telle relation ne peut pas avoir lieu. Alors pourquoi, quelle est la raison pour laquelle elle ne peut pas avoir lieu ? Eh bien parce qu'en fait, il y a un groupe, qu'on appelle le groupe de Galois, qui permute les racines entre elles, qui n'est jamais trivial, pour une équation irréductible, celle-là est irréductible, qui permute les racines entre elles, et qui a la propriété de préserver toutes les relations algébriques rationnelles entre les racines. Donc si cette relation avait lieu, comme vous pouvez remplacer E par n'importe quelle autre racine, toutes les racines seraient positives, puisqu'un carré c'est positif, 4 c'est positif, 2 c'est positif, donc toutes les racines seraient positives, ce n'est pas possible.

Donc on sait, a priori, simplement parce qu'il y a ce groupe d'ambiguïté, ce groupe de symétrie qui est caché derrière, qu'il est impossible que cette relation ait lieu. Alors en l'occurrence, le groupe est très très simple, parce que j'ai pris une équation cyclique, et en fait c'est très facile, c'est un petit exercice qui prend 3 secondes, de vérifier que si vous avez une racine de cette équation, si vous prenez son carré moins 2, c'est encore une racine de l'équation. Donc vous avez un groupe d'invariance qui fait que, automatiquement, à chaque fois que vous avez une racine x, la formule $x^2 - 2$ vous donne une autre racine.

Alors quel est l'intérêt de ça ? L'intérêt, ça veut dire que toutes les racines de cette équation sont fonctions rationnelles d'une seule des racines ; et comme c'est le cas, si vous avez une relation algébrique entre les racines, comme la relation qui était là, vous en déduirez que sur une racine quelconque, vous avez une relation polynomiale, mais c'est forcément un multiple du polynome irréductible dont on est parti, et on a la conclusion. Alors on verra ce raisonnement en un petit peu plus de détails, mais que dit la théorie de Galois dans ce cas là ? Eh bien, elle dit qu'en fait, il faut indexer convenablement les racines de l'équation, pas du tout comme ABCD comme on avait fait tout à l'heure, il faut les indexer, les racines, par les entiers modulo 5, exactement comme j'ai indiqué sur la figure, donc 0, 1 pour les deux premières, les plus à gauche, 3, 4 pour les deux qui suivent, et puis 2 pour celle qui est le plus à droite. Et si vous faites ça, vous allez voir qu'en fait le groupe de Galois a décelé une structure qui était cachée, qui était sous-jacente aux racines, et qui était la structure, si vous voulez, des entiers modulo 5. Et le groupe de Galois les permute de manière cyclique, mais cette structure, elle est présente, et on ne l'aurait jamais vue si on avait simplement agi comme, disons, comme un expérimentateur ou un physicien en disant, eh bien j'ai une équation, j'ai ses racines, et puis je suis content.

En fait, ce qui est extraordinaire dans la théorie de Galois, c'est que derrière cette évidence apparente, si vous voulez, qui vous donne une équation et qui vous fait voir ses racines, il y a une théorie beaucoup plus subtile, beaucoup plus intéressante qui est cachée derrière, et qui justement permet de comprendre, de saisir qu'il y a, du fait que l'équation est irréductible et du fait qu'elle n'est pas résoluble directement, qu'elle n'est pas factorisée, il y a une ambiguïté entre les racines. Alors en fait, pour mieux comprendre tout ça, donc il y a une définition abstraite, on va la voir telle que l'écrit Galois, donc on va voir qu'il y a une subtilité, que Galois décrit absolument de manière parfaite, et qu'il faut comprendre, sinon on ne comprend pas la théorie. Donc soit une équation donnée, on prend les racines, ce que dit Galois c'est qu'il y aura toujours un groupe de permutation des lettres qui aura la propriété suivante : que toute fonction des racines invariable par les substitutions de ce groupe soit rationnellement connue et réciproquement que toute fonction des racines qui est déterminable rationnellement soit invariable par ces substitutions.

Alors si on le dit comme ça, on ne comprend pas vraiment si on n'a pas l'explication de Galois. Voilà le texte de Galois est beaucoup plus précis et beaucoup plus intéressant que cet énoncé abstrait. Voilà ce que dit Galois.

Il dit ici la chose suivante :

> “*Nous appelons ici invariable, non seulement une fonction dont la forme est invariable par les substitutions des racines entre elles* (voyez bien si on prend la somme des racines, par exemple, elle est invariable par toutes les substitutions), *mais encore celle dont la valeur numérique ne varierait pas par ces substitutions.* Et là, il y a une distinction qui est cruciale. Par exemple, ce que dit Galois, c'est que si l'équation c'est $Fx = 0$, eh bien Fx c'est une fonction des racines qui ne varie par aucune permutation. En fait, il est beaucoup plus précis que ça, il continue et il dit : *Lorsqu'une fonction des racines ne change pas de valeur numérique par une certaine substitution opérée entre les racines, elle est dite invariable par cette substitution.*
>
> *On voit qu'une fonction peut très bien être invariable par telle ou telle substitution entre les racines sans que sa forme l'indique. Ainsi si* $Fx = 0$ *est l'équation proposée, la fonction* $\varphi(F(a), F(b), F(c), ...)$ (on épèle les racines), *où* φ *est une fonction quelconque, rationnelle bien sûr, sera une fonction de ces racines qui sera invariable par toute substitution entre les racines, sans bien sûr que sa forme l'indique.*

Ça pourrait être par exemple $F(a) + 3F(b)$ ou un truc comme ça. Or c'est une question dont il ne paraît pas qu'on ait encore la solution de savoir si étant donnée une fonction de plusieurs quantités numériques, on peut trouver un groupe qui contiennent toutes les substitutions par lesquelles cette fonction est invariable et qui n'en contiennent pas d'autres.

Vous voyez, il y a un pas énorme qui est franchi à ce moment-là, parce que dans Lagrange par exemple, ou dans d'autres textes, on cherchait à trouver pour l'équation générale, des fonctions des racines qui ne sont pas trop invariantes, tout en étant un petit peu invariantes. Par exemple si vous prenez une équation du quatrième degré, vous avez $ab + cd$, ça c'est une fonction qui n'est pas invariante par toutes les permutations mais qui ne prend que trois valeurs différentes quand on applique toutes les permutations et ça permet de résoudre l'équation du quatrième degré par l'équation du troisième degré. Donc c'était différent, les gens faisaient des choses dans le cadre complètement général.

Alors donc ce que dit Galois c'est qu' :

> *évidemment, cela a lieu pour des quantités littérales, puisqu'une fonction de plusieurs lettres invariable par deux substitutions est invariable par leur produit.* Donc ça c'est évident. *Mais rien n'annonce que la même chose ait lieu quand aux lettres, on substitue des nombres*, ce n'est absolument pas évident. Il dit : *on ne peut donc point traiter toutes les équations comme des équations littérales, il faut avoir recours à des considérations fondées sur les propriétés particulières de chaque équation numérique, c'est ce que je vais tâcher de faire.*

Il faut voir qu'à l'époque les gens faisaient énormément de calculs et par exemple si vous regardez la copie de Galois d'entrée à l'École Préparatoire, vous verrez qu'on donnerait ces problèmes même à des gens maintenant, je ne suis pas sûr qu'ils seraient tous capables de donner la bonne solution. Et donc les gens faisaient énormément de calculs et remarquons que tout ce qu'une équation numérique peut avoir de particulier doit provenir de certaines relations entre les racines. Ces relations seront rationnelles dans le sens que nous l'avons entendu, c'est à dire qu'elles ne contiendront d'irrationnels que les coefficients de l'équation bien sûr et les quantités adjointes.

> *De plus ces relations ne devront pas être invariables par toute substitution opérée entre les racines, sans quoi on n'aurait rien de plus que pour les équations littérales ordinaires. Ce qu'il importe donc de connaître, c'est par quelles substitutions peuvent être invariables les relations entre les racines, ou ce qui revient au même, des fonctions des racines dont la valeur numérique est déterminable rationnellement.*

Alors là je vais quand même vous donner une toute petite explication. Ce qui est incroyable c'est la chose suivante, c'est que ce que fait le groupe de Galois, c'est, si vous voulez, si on vous disait, je prends une équation, il faut déterminer toutes les relations rationnelles entre les racines, vous pourriez le faire, on va voir comment. Mais qu'est ce que ça vous donnerait ? Ça vous donnerait les multiples d'un polynôme, qu'on appelle le polynôme associé à l'extension galoisienne correspondante, ce serait quelque chose qu'il est très difficile de calculer et de manipuler. Et ce qui est merveilleux, c'est que ce que Galois a démontré, c'est que ce n'était pas exactement les relations, une certaine fonction comme par exemple tout à l'heure $E - 4B^2 - 2C^2 = 0$ ou un truc comme ça, ce n'est pas ça qui compte. Ce qui compte, ce n'est pas un truc égal à 0, parce que les trucs égaux à 0, vous auriez un peu de mal à les déterminer, ce qui compte, ce sont les quantités rationnelles, c'est-à-dire que bien sûr que si vous écrivez une relation égale à 0, 0, c'est rationnel, donc elle doit être invariante par le groupe de Galois. Mais réciproquement, si vous prenez une expression qui est invariante par le groupe de Galois, elle ne vous donnera pas 0, mais elle vous donnera un nombre rationnel. Mais comme ce nombre est rationnel, vous pouvez le soustraire de cette expression et vous obtenez 0. Donc, par l'invariance par le groupe, vous déterminez toutes les relations rationnelles, donc toute la spécificité d'une équation. Et alors donc, ce que fait Galois, le groupe de Galois, donc en fait, il donne un groupe de permutations des racines, qui est toujours non trivial, c'est ça qui est absolument époustouflant, c'est que le groupe n'est jamais réduit à l'identité, sauf si l'équation est bien sûr complètement résolue, c'est à dire si on a un facteur irréductible de degré 1. Et pour montrer l'existence de ce groupe d'ambiguïté, Galois procède en deux étapes ; la première étape, c'est de trouver une autre équation (ça en fait, le rapport de Poisson dit que Lagrange le savait déjà), de trouver une équation auxiliaire telle que les racines de l'équation dont on part soit toutes fonctions rationnelles d'une seule racine de l'équation auxiliaire. Et de plus (bien sûr, ça s'en déduit immédiatement), que les racines de l'équation auxiliaire vont être fonctions rationnelles les unes des autres. Donc les racines de cette équation, c'est un peu comme dans l'équation de tout à l'heure, quand vous aviez la transformation $x \to x^2 - 2$, vous avez des transformations rationnelles qui vont transformer les racines les unes en les autres. Et alors après, c'est fini parce que si vous prenez une relation rationnelle entre les racines, elle va vous donner une équation $H(V) = 0$, qui va pouvoir se formuler en termes d'une seule racine de l'équation auxiliaire. Comme il y a une seule racine de l'équation auxiliaire, elle sera forcément un multiple du polynôme minimal de V et vous avez gagné, puisque ce polynôme minimal est invariant par les transformations rationnelles. Donc la démonstration est incroyablement simple, bien sûr. Alors c'est ce qu'on voit, le groupe de Galois, il le calcule de manière explicite. Il dit, bien sûr, la difficulté des calculs ; il n'avait pas d'ordinateur, à l'époque, et on va voir à quoi ressemble la difficulté des calculs, je vais vous le montrer, parce que maintenant, on n'a pas d'excuse pour ne pas le montrer. Donc voilà ce que Galois disait, et c'était vraiment quelque chose d'extrêmement profond parce qu'il ne dit pas qu'il ne faut pas faire les calculs, il dit :

> "*sauter à pieds joints sur les calculs, grouper les opérations, les classer* (justement) *suivant leurs difficultés et non suivant leur forme, telle est selon moi la mission des géomètres futurs*".

Donc alors maintenant, si vous voulez, on va voir un peu plus tard comment Galois faisait les calculs, mais avant de vous montrer ça, je vais vous montrer simplement comment on fait maintenant, pour comprendre ce que c'est que le groupe de Galois de manière extrêmement naturelle et simple il y a un théorème qui est un théorème de Chebotarev et qui permet de comprendre en quel sens il est vrai que plus le groupe d'ambiguïté est grand plus il est difficile de résoudre une équation. Alors comment est ce que le théorème est formulé ? Eh bien, le théorème est formulé en disant qu'on va s'intéresser maintenant (l'équation est à coefficients entiers), donc on va pouvoir réduire modulo un nombre premier, c'est-à-dire que pour chaque nombre premier, on va regarder si on peut résoudre l'équation modulo ce nombre premier ; ce n'est pas très difficile de savoir ce que ça veut dire : ça veut dire que tous les nombres qui sont multiples d'un nombre premier p, vous les identifiez à zéro et vous cherchez à résoudre l'équation. Ce que dit le théorème de Chebotarev, c'est que la probabilité pour que l'équation soit résoluble modulo un nombre premier p, la probabilité sur l'ensemble des nombres premiers, c'est l'inverse de l'ordre du groupe de Galois, donc c'est quelque chose qui est extrêmement simple, et si vous regardez par exemple pour le polynôme dont je vous ai parlé tout à l'heure et si vous le réduisez modulo p, alors vous aurez l'impression qu'il change chaque fois mais c'est parce que quand il y a un moins quand vous réduisez modulo p par exemple si vous réduisez modulo 47, 44 ça fait -3, donc ça vous donne une impression, mais vous voyez qu'il arrive, assez fréquemment là, que le polynôme ait toutes ses racines dans les entiers modulo le nombre premier. Alors, il ne faut pas vous inquiéter du nombre 11, le nombre 11, il a la propriété que ce qu'on appelle le discriminant de l'équation dans les parties, je crois que c'est 11 puissance 4 ou quelque chose comme ça, donc en fait ça veut dire que le nombre 11 est très particulier et l'équation, elle n'aura pas des racines distinctes, quand on travaille modulo 11. Par contre, dès qu'on prend des nombres premiers autres, si les racines existent dans les entiers modulo p, elles vont être distinctes et alors là, on voit un comportement qui est très très clair, et qui vous dit qu'à peu près tous les cinq nombres premiers, l'équation est complètement résolue, elle est complètement résolue, elle a toutes ses racines modulo p.

Donc cette équation, elle est facile : elle est facile au sens où si après, vous regardez la densité, vous voyez, j'ai mis l'inverse de la densité ici, et on voit bien qu'on obtient le nombre 5, on obtient le nombre 5 en prenant... on va très loin au niveau... l'indice qui est en bas le 10 000, ça veut dire qu'on est au dix millième nombre premier et on regarde l'inverse de la proportion de nombres premiers pour lesquels elle est complètement résolue. Alors c'était une équation très simple. Maintenant, on va s'intéresser à des équations un petit peu plus compliquées. Donc prenons par exemple les racines cinquième de 2 : si vous regardez les racines cinquièmes de 2 et si vous essayez modulo un nombre premier, eh bien là, vous allez vous apercevoir que bouh...! Dans tous les exemples que je vous ai montrés, il n'y en a même pas un seul dans lequel l'équation est vraiment résoluble complètement modulo le nombre premier et je suis pourtant allé assez loin. Et alors si vous faites le calcul, vraiment, si vous faites le calcul loin, vous allez vous apercevoir que l'inverse de la densité de l'ensemble des nombres premiers pour lesquels il y a cinq solutions, cinq racines cinquième de 2, vous voyez que ça vaut environ 20 ; ça met du temps à se stabiliser mais au bout d'un moment, ça se stabilise et ça vaut de l'ordre de 20. Donc qu'est ce que ça veut dire ? Ça veut dire que le groupe de Galois de cette équation, il est d'ordre 20 ; bien sûr, je vais dire, il y a des gens naïfs, quand ils restituent la théorie de Galois, ils vous disent $x^5 = 2$, c'est un groupe cyclique, bien sûr, ce n'est pas ça : c'est un groupe d'ordre 20, qui est un petit peu plus compliqué qu'un groupe cyclique, parce que pour obtenir un groupe cyclique il aurait fallu adjoindre les racines cinquième de 1 et on ne l'a pas fait. Alors on peut faire le calcul explicite de ce groupe, je vous montrerai comment Galois le faisait, et quand on fait le calcul explicite, on s'aperçoit, bien sûr, qu'il y a la permutation cyclique, mais qu'il y a aussi d'autres permutations, qui sont même impaires ; en fait, le fait que ce groupe ait des permutations impaires, je pense que c'est la raison qui a fait croire à Abel et à Galois qu'ils avaient résolu l'équation du cinquième degré, je pense que je vous dirai pourquoi un petit peu plus tard, et en fait donc, à nouveau, il y a une structure sous-jacente, et ce qu'il faut faire, c'est indexer les racines sur le corps $\mathbb{F}_5$ mais le groupe de Galois, vous voyez dans ce cas-là, ça devient le groupe affine, ce n'est plus le groupe seulement des translations, c'est le groupe affine, c'est le groupe à nouveau sur le corps $\mathbb{F}_5$, mais des transformations affines de la forme x donne $ax+b$, qui sont effectivement très simple, mais il faut indexer les racines, de manière évidente, c'est 0 1 2 3 4 par le corps $\mathbb{F}_5$.

Alors regardons maintenant un exemple d'ordre 10, c'est un exemple qui est plus intéressant. Donc je vous donne une équation, dont le groupe dihédral est le groupe de Galois, c'est un groupe qui est d'ordre 10 et on la trouve facilement en regardant par exemple le théorème de Chebotaref, on obtient ça et alors si on regarde cette équation, si on fait le calcul explicite de son groupe de Galois, on trouve, à ce moment-là, quelque chose d'un petit peu différent. Alors, vous voyez qu'on a le même type de permutation cyclique quand j'écris les petits ronds, là, ce sont les racines dans le plan complexe, je n'ai pas fait ça de manière arbitraire, les petits ronds sont les racines dans le plan complexe. Et les permutations, ce sont de vraies permutations du groupe de Galois. Donc on a la permutation du haut, qui est une permutation cyclique entre les cinq racines, et la permutation du bas, qui est caractéristique du groupe dihédral parce que c'est une involution, bien sûr avec un point fixe, mais qui quand on les met ensemble, l'une avec l'autre, va engendrer un groupe dihédral. Alors la structure sous-jacente à nouveau, eh bien on voit bien qu'à nouveau on va indexer les racines de la manière que j'ai indiquée 0 1 2 3 4 d'accord, par le corps $\mathbb{F}_5$ et à nouveau, le groupe de Galois est un sous-groupe du groupe affine. Alors donc maintenant, l'équation vraiment intéressante si on s'en était restreint au degré 4, on n'aurait pas eu d'équation intéressante parce qu'on n'aurait eu que des équations qui sont résolubles par radicaux.

C'est pour ça que j'ai choisi le degré 5, bien sûr, c'est pour pouvoir vous montrer une équation qui soit non résoluble par radicaux. Alors, j'ai quand même fait un choix un peu simplificateur c'est-à-dire que j'ai pris une équation dont le discriminant est un carré, de telle sorte que son groupe de Galois, ce ne soit pas le groupe symétrique, vous voyez, si vous me donnez... tout à l'heure, vous pourrez me donner une équation au hasard, et je vous montrerai que son groupe de Galois, c'est le groupe symétrique S_5. Mais, avec un peu de chance, on arrive à... donc dès que le discriminant est un carré, c'est une espèce d'ersatz de ce qui se passait pour l'équation du second degré, le groupe de Galois devient le groupe A_5, qui est un groupe simple, qu'on appelle le groupe alterné, et on le voit en calculant la probabilité pour que l'équation soit résoluble complètement modulo p.

Voyez cette probabilité, si vous allez assez loin, vous voyez que l'inverse de cette probabilité, c'est

60. Alors si on fait le calcul explicite, on peut calculer explicitement le groupe de Galois, on trouve des permutations comme celles qui sont là. Quel est l'intérêt des deux permutations que j'ai écrites ? Eh bien, c'est qu'elles vont vous donner la présentation du groupe. Vous voyez, c'est un groupe d'ordre 60, donc un groupe d'ordre 60, ça peut paraître difficile à appréhender, en fait il est extrêmement simple à appréhender, parce que c'est un groupe dont la présentation est très simple ; il y a un générateur, celui du haut, qui est de carré 1 ($u^2 = 1$) et celui du bas, son cube est égal à 1 ($v^3 = 1$), c'est évident puisqu'il permute de manière cyclique les trois racines qui sont là, et en plus, quand on fait le produit uv de ces deux générateurs, on obtient un élément dont la puissance cinquième est égal à 1 ($(uv)^5 = 1$).

Alors quand vous connaissez ces relations $u^2 = 1, v^3 = 1, (uv)^5 = 1$, vous avez tout compris sur le groupe parce qu'après vous écrivez des mots avec les lettres u et v, et vous faites les simplifications qui s'imposent, c'est-à-dire les simplifications qui viennent de $u^2 = 1$, vous ne pouvez pas répéter u deux fois, $v^3 = 1$, vous ne pouvez pas répéter v 3 fois, et ainsi de suite. Et il est immédiat, par exemple, qu'une équation, qui a ce groupe-là, ne peut pas être résoluble par radicaux parce qu'à ce moment là, vous pourriez représenter ces relations de manière abélienne, c'est-à-dire de manière commutative, mais si vous avez $u^2 = 1, v^3 = 1$ et si u et v commutent, quand vous prenez $(uv)^5 = 1$, vous allez en déduire immédiatement que $u = v = 1$; donc vous avez une contradiction évidente. Donc c'est comme ça qu'on comprend ces groupes.

Et maintenant, ce qui est extraordinaire, c'est que quand Galois avait 18 ans, il a publié un article, son article est publié dans le Bulletin de Férussac, en juin 1830, et dans cet article, il fait la chose suivante : je vous ai montré sur des exemples très simples qu'il fallait indexer les racines par le corps $\mathbb{F}_5$ d'accord, alors ce que fait Galois, c'est fantastique, il définit les corps finis quelconque $\mathbb{F}_q$, bon, on sait qu'il faudrait être beaucoup plus "non canonique" que ça, il y a une ambiguïté dans la définition du corps $\mathbb{F}_q$, mais donc il définit le corps $\mathbb{F}_q$ (Gauss le connaissait sûrement aussi) et ensuite, qu'est ce que fait Galois ? Bien sûr, il calcule le groupe de Galois de $\mathbb{F}_q/\mathbb{F}_p$, ce n'est pas difficile, il est engendré par le Frobenius.

Ce n'est pas ça qui est difficile ; ce qui est extraordinaire, c'est que Galois prolonge au cas général des équations résolubles par radicaux ce qu'il avait compris pour les équations de degré premier en utilisant le corps $\mathbb{F}_q$. Voilà ce qu'écrit Galois. Alors vous ne le lirez pas, mais ça ne fait rien, je crois que je peux le lire : alors il dit la chose suivante "*Cette remarque...*" Donc qu'est ce qu'il fait ? C'est dommage que je ne voie pas la formule mais elle est dans l'article. Qu'est ce qu'il dit ? Il dit "*vous prenez une équation*" bon vous savez, vous voulez qu'elle soit résoluble, il demande qu'elle soit primitive, c'est une petite condition qui n'est pas difficile à comprendre, qui dit en gros que le corps qui est défini par l'équation n'a pas de sous-corps. Donc il prend son équation, ensuite il dit que "*si l'équation est résoluble (si elle est primitive), on pourra indexer les racines non pas par* $\mathbb{F}_5$ *comme tout à l'heure, mais par un corps fini* $\mathbb{F}_q$ *et que les transformations des racines par le groupe de Galois seront automatiquement contenues...*" dans quoi ? Pas seulement dans le groupe affine, ce serait trop simple, si c'était comme dans les cas précédents, le groupe $ak + b$ comme dans le cas premier, non, *"...dans le groupe affine produit semi direct par les puissances du Frobenius"*.

Donc ça, c'est vraiment extraordinaire, c'est écrit explicitement dans l'article de Galois et Galois avait la démonstration, il y a quelques cas particuliers auxquels il faut faire attention. Mais donc il avait parfaitement compris ce qui se passait dans cette chose-là.

Bien sûr, après, il explique la théorie générale, mais on réduirait à très peu la théorie de Galois si on ne parlait que de la théorie générale. En général, si vous voulez, quand on explique la théorie de Galois, quand on explique ce qu'a fait Galois, on explique surtout la théorie générale, qui est expliquée ici, par exemple, si on adjoint à une équation donnée, la racine d'une équation auxiliaire irréductible, qu'est-ce qui arrive, etc. Mais, en fait, la théorie de Galois, Galois était allé bien plus loin, au sens où il avait compris que, quand on connaît le groupe de Galois d'une équation dans le cas où elle est résoluble, ce groupe, en fait, décèle une structure très intéressante, très particulière dans les racines, par le fait qu'on peut indexer ces racines par tous les éléments d'un corps fini, et qu'ensuite, si vous voulez, cette structure est automatiquement préservée par l'action du groupe de Galois.

Donc, c'est une structure intrinsèque à l'ensemble des racines. C'est quelque chose qui est tout à fait extraordinaire. Alors, je ne vais pas vous embêter avec ça.

Ce que je vais faire maintenant, c'est vous montrer les calculs. J'espère que vous ne m'en voudrez pas. À l'époque de Galois, les gens ne pouvaient pas faire les calculs.

Bon, ça, c'est des trucs classiques, je n'ai pas envie. Donc, alors ça, ce n'est pas grave, ce n'est rien. C'était pour montrer un peu Chebotarev.

Vous voyez, si vous calculez, pour savoir quel groupe de Galois a une équation, vous prenez l'inverse de cette proportion de tout à l'heure. Donc, vous voyez, pour le polynôme qui est là, vous avez 60. Là, vous avez 5. Là, vous avez 10.

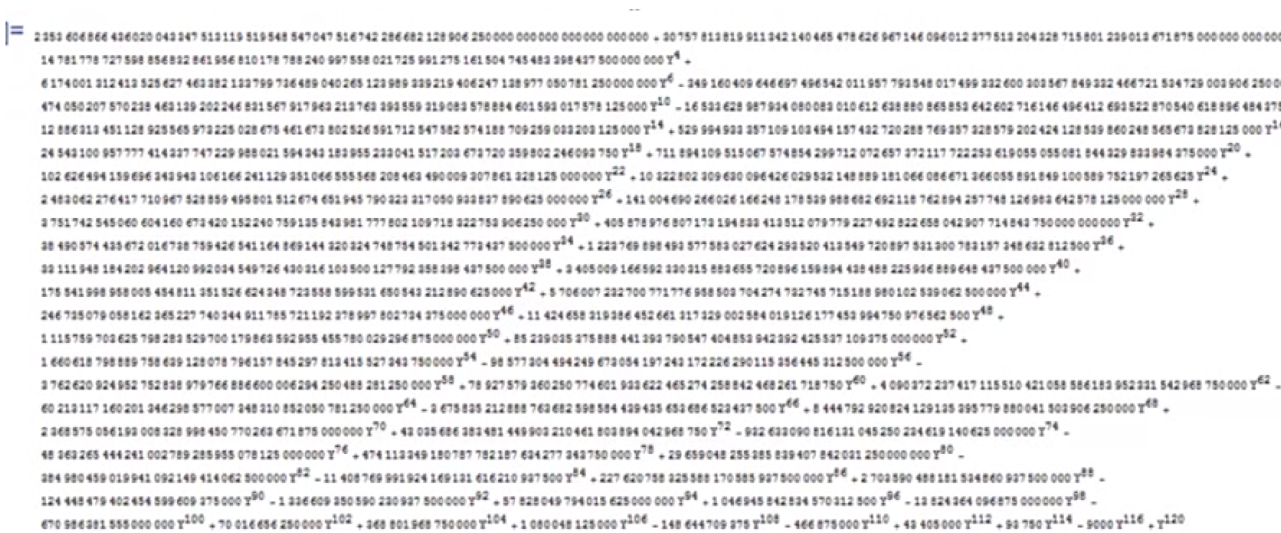
Et là, vous avez 20. Donc, ça vous donne le point de départ. Bon.

Alors ensuite, on part d'une équation. On part, par exemple, de celle-là. Celle-là, c'est celle qui a 10. Donc, c'est celle qui a le groupe dihédral. D'accord ? Alors, qu'est-ce qu'on fait quand on a une équation ? Comment on fait pour calculer son groupe de Galois ? Comment Galois proposait de le faire ? Alors, ce que disait d'abord Galois, c'est que vous allez trouver une fonction des racines qui est telle que cette fonction va prendre factorielle 5 valeurs différentes, 120 valeurs différentes, quand vous permutez les racines entre elles. Alors, on essaye la fonction la plus simple possible. La fonction la plus simple possible, c'est $a + 2b + 3c + 4d$. Je n'ai pas envie de mettre e, puisque la somme des racines est connue. Et puis, les coefficients, il faut bien qu'ils soient différents. Donc, j'ai pris 1, 2, 3, 4. Ça ne peut pas être plus simple que ça. D'accord ? Donc, on prend ces coefficients-là et on cherche quelle est l'équation qui a pour racine les $a+2b+3c+4d$. D'accord ? On la calcule.

Je ne vous la montre pas parce que ça vous ferait peur. Si quelqu'un veut que je la montre, je peux la montrer. D'accord ? Mais bon, il ne faut peut-être pas.

Ce qui est sûr, c'est que vous demandez de la factoriser. Si, je vais quand même vous la montrer. D'accord ? Attendez, je vais supprimer.

Je vais vous la montrer. Je vais faire “entrez”. Vous voyez ? Voilà.



D’accord ? Ce n’est pas jojo. D’accord ? Donc, si on vous donne comme exo de factoriser ce polynôme, bon, ça peut être un peu embêtant. L’ordinateur, il fait ça en 3 secondes.

D’accord ? Je vais lui demander de le faire, l’ordinateur, parce que pourquoi pas. Voilà. Donc, l’ordre que je lui donne, c’est de factoriser ce polynôme.

D’accord ? Il va le faire. Voilà. Il vous donne le résultat tout de suite.

Donc, vous voyez que tous les facteurs irréductibles sont de degré 10. D’accord ? Il y en a 12. Et maintenant, une fois qu’on a ces facteurs irréductibles, par un raisonnement d’élimination qui est très très simple, on peut exprimer les racines de l’équation de départ en fonction d’une racine quelconque de ce polynôme.

Alors, on fait le calcul. C’est un calcul par élimination qui n’est pas difficile, mais qui est long. Et on obtient, voilà, l’expression pour les racines. C’est une expression qui est unique. Vous voyez qu’elle... Ici, ça s’arrête au degré 8. Ici, ça s’arrête au degré 9. On ne va pas jusqu’au degré 10, puisque l’équation irréductible est de degré 10. Donc, on peut toujours simplifier par y^{10}. Donc, voilà ces fonctions-là. Ça, c’est tout à fait calculable. Je veux dire, Galois peut le faire parfaitement, ça. Il n’y a aucune difficulté, là, sauf le premier polynôme. Ensuite, on prend les racines du polynôme du premier facteur, là, de tout à l’heure, qui était celui-là, d’accord ? On choisit le premier facteur irréductible. On prend ses racines. Elles ont l’air de ça. Et alors, maintenant, ce qui est incroyable, c’est que chaque fois qu’on a un couple de racines... C’est ça qu’il faut bien comprendre. Chaque fois qu’on a un couple de racines de l’équation auxiliaire, ça va nous donner une permutation. Ça correspondait au tableau de tout à l’heure, qui donnait l’ambiguïté entre les racines. Alors, j’ai écrit un petit programme qui va vous montrer que chaque fois que vous me donnez deux nombres, par exemple celui-là, j’ai une permutation correspondante. Dans ce cas-là, on va voir apparaître le groupe dihédral.

En fait, on peut fixer l'une des deux. On va, par exemple, fixer la première racine comme étant égale à 1. Et on va faire varier la deuxième. Et on va voir qu'en faisant varier la deuxième, on obtient tout le groupe dihédral.

Alors, j'obtiens l'identité, mais je ne l'ai pas marquée. Ensuite, on obtient ça. Vous voyez bien que ça fait partie du groupe dihédral.

Ça, c'est une involution de carré 1 qui fixe ce point, etc. Et puis, on va avoir les dix éléments. Ça, c'est une permutation cyclique.

Là, on a une involution qui fixe un autre point, une autre involution, permutation cyclique, involution, etc. D'accord ? Permutation cyclique, involution. D'accord.

Donc, je veux dire, là, on voit parfaitement comment le groupe de Galois se calcule. Le calcul n'est pas vraiment compliqué, parce que l'équation a pour groupe le groupe dihédral. Et ensuite, si on applique la factorisation de tout à l'heure, on peut vérifier quelque chose qui est mieux encore, enfin, qui est mieux, qui est très relié au théorème de Chebotarev et qui est un théorème de Dedekind. Et qui dit que si on regarde maintenant comment le polynôme va se factoriser modulo p, par exemple modulo 23, ça va correspondre à des cycles dans le groupe de Galois. Vous voyez, par exemple, la décomposition modulo 23, elle va correspondre à une involution qui va fixer une racine, qui va permuter deux autres racines, qui va permuter deux autres racines, et ainsi de suite.

Ça, ça va correspondre à une permutation cyclique. Et ça, ça va correspondre à une involution. Voilà.

Donc, en fait, on a un contrôle. Alors là, maintenant, on va partir d'une autre équation. Ah oui, c'était celle dont j'étais parti. Et si je prends celle dont j'étais parti au départ. Celle-là, on l'a déjà complètement traitée. Elle avait un groupe de Galois qui était très simple.

Mais vous voyez qu'on va retrouver cette simplicité du groupe de Galois parce que quand on factorise le polynôme associé, eh bien, on va ne retrouver que des tout petits polynômes de degré 5. Donc là, le groupe de Galois est d'ordre 5. Il est très, très simple. On peut calculer l'expression des racines. On peut calculer le polynôme associé.

Mais l'intérêt, maintenant, par rapport à ce qu'on avait tout à l'heure, c'est qu'on peut calculer explicitement les permutations. Ça, c'est beaucoup plus joli que de savoir abstraitement que le groupe de Galois est d'ordre 5. Par exemple, ici, on va obtenir toutes les permutations. Et ces permutations ne se comprennent qu'une fois qu'on a indexé, comme je l'ai dit tout à l'heure, correctement les racines par le corps $\mathbb{F}_5$ de telle sorte qu'elles deviennent simplement des translations.

On a une structure qui est dévoilée par le groupe de Galois. De même qu'on l'a vu, il y a la résolubilité modulo un nombre premier. Ça, on l'a déjà montré tout à l'heure.

Maintenant, on regarde l'équation des racines $5^{\text{ièmes}}$. Bon alors l'équation des racines $5^{\text{ièmes}}$, c'est un petit peu plus embêtant. Voilà le polynôme de degré 120 dont on part.

Les polynômes irréductibles qu'on obtient ne sont pas très méchants. Ils sont de degré 20. Ils ne sont vraiment pas méchants du tout.

Et à nouveau, les équations qui donnent les racines en fonction de ces polynômes ne sont pas compliquées. Regardez, celle-là est extrêmement simple. Je vais faire un petit aparté pour les mathématiciens.

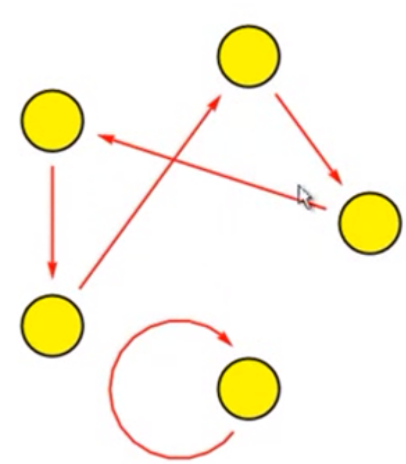
Vous savez, en mathématiques, on a un moyen merveilleux pour résoudre une équation. Si on prend l'anneau des polynômes, on a une équation $P(x) = 0$. Pour résoudre l'équation, on prend l'anneau des polynômes et on le divise par l'idéal engendré par $P(x)$. À ce moment-là, on a résolu l'équation parce que x est une racine. Malheureusement, ça a un gros inconvénient de faire ça, c'est qu'en général, on a une seule racine.

C'est-à-dire que vous ne pouvez pas factoriser le polynôme. Mais la méthode de Galois, la méthode dont je vous parle, elle permet de factoriser entièrement le polynôme. Et c'est formidable, après, quand on a un peu l'habitude de l'ordinateur, de voir que quand on a exprimé toutes les racines en fonctions rationnelles d'une seule racine, on peut se poser toutes sortes de questions et on a une réponse absolument immédiate.

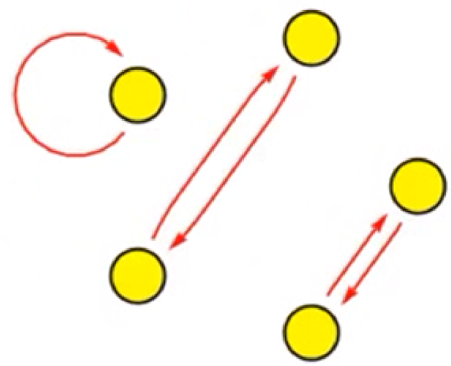
C'est quelque chose de merveilleux. Donc, il y a un pas qui a l'air de rien. Bien sûr, quand on définit les nombres complexes, on a rajouté toutes les racines de l'équation parce qu'on a rajouté i, mais l'autre racine, c'est $-i$. Lorsqu'on définit les corps finis, c'est pareil.

Mais lorsqu'on définit des extensions plus générales, ce procédé-là est extrêmement efficace. Maintenant, ce qui se passe, c'est que là, on fait pareil. On regarde les racines de l'équation auxiliaire et on a le groupe de Galois.

Vous allez avoir le groupe de Galois. Il est un petit peu plus compliqué parce qu'il est d'ordre 20. Vous avez des permutations cycliques. Ça, c'est encore le groupe dihédral. Je vais essayer de trouver quelque chose qui ne soit pas dans le groupe dihédral, quand même. Ça, c'est encore dans le groupe dihédral. Ça encore. Ça encore. Tiens, c'est bizarre. On va aller vers le bas. Ça encore.



Voilà, ça, ce n'est pas dans le groupe dihédral. Ça, c'est une permutation impaire. Il faut bien savoir maintenant, si vous réfléchissez, si le groupe A_5 avait contenu le groupe des transformations affines, l'équation du cinquième degré aurait été résoluble par radicaux.



Je pense que c'est ça l'erreur qu'ont fait Galois et Abel. Et la raison, c'est la suivante. C'est que le polynôme adjoint, pour résoudre l'équation, aurait été un polynôme de degré 3, puisque 60 divisé par 20, ça vaut 3. Et à ce moment-là, on aurait pu résoudre cette équation puisqu'elle est de degré 3. Et comme le groupe d'ordre 20 est résoluble, on aurait pu, en rajoutant des radicaux, résoudre l'équation de départ. Mais c'est bien sûr faux. Il suffit de regarder que la permutation qui est en face de vos yeux, elle est impaire. Elle n'est pas paire. Et donc, elle ne peut pas appartenir au groupe A_5. Donc, voilà ce qui se passe. Alors, bien sûr, il y a le théorème de Chebotarev.

Vous pouvez aussi regarder ce qui se passe ici. D'accord ? Bon. Alors maintenant, on va venir à quelque chose de beaucoup plus intéressant.

Et je pense que c'est ce à quoi Galois faisait référence lorsqu'il disait "*on ne peut pas faire les calculs*". Pourquoi ? Parce que ça ne l'intéressait pas d'avoir des équations qui étaient résolubles par radicaux. Il y en avait partout.

Il voulait une équation concrète, numérique, qui ne soit pas résoluble par radicaux. Ça, il le voulait absolument, d'accord ? Et appliquer sa méthode à cette équation.

Alors, j'en ai pris une qui, comme je l'ai dit tout à l'heure, a un discriminant qui est un carré. Donc, elle n'est encore pas trop méchante. Ça veut dire que quand vous prenez son polynôme irréductible, bon, c'est celui-là, il va se casser en deux.

Il va se casser en deux. Est-ce que je l'ai cassé en deux ? Voilà. Non, je ne l'ai pas cassé en deux, peu importe. Vous avez un polynôme de degré 60. Je ne sais pas si le degré de celui-là, c'est 60. Oui, c'est 60. Donc, celui-là, c'est le polynôme irréductible, de degré 60, que vous obtenez en décomposant le polynôme associé toujours aux racines $a + 2b + 3c + 4d$, en facteurs irréductibles. Donc, vous obtenez ça.

Et alors maintenant, vous demandez de calculer les racines comme tout à l'heure. Vous vous souvenez, tout à l'heure, il y avait une belle formule pour les racines de l'équation de départ en fonction du polynôme associé, des racines du polynôme associé. Alors maintenant, vous demandez de faire le calcul.

Alors ça, vous pouvez le demander à l'ordinateur. Il fait le calcul. Il obtient des polynômes. Il obtient des polynômes de degré 59, puisque l'équation associée est de degré 60. Et alors, l'ordinateur fait les calculs avec, sans aucune difficulté. Mais par curiosité, j'ai demandé à l'ordinateur de me donner le terme constant du polynôme qui donne la première racine.

D'accord ? Le terme constant, c'est cette fraction-là. D'accord ? Alors, j'ai demandé à l'ordinateur le numérateur de la fraction. C'est facile.

Et j'ai demandé combien il y avait de zéros. C'est 10 puissance 393. Alors maintenant, les physiciens nous disent que c'est le nombre d'univers qui sont possibles, 10 puissance 500, un truc comme ça.

Mais vous imaginez bien que quand on doit faire des calculs à la main, et que pour la première racine, et le terme constant, on obtient ce terme-là, c'est impossible. C'est absolument impossible de continuer. C'est impossible.

C'est infaisable. C'est infaisable. À la main, c'est infaisable.

À l'ordinateur, c'est parfaitement faisable. C'est-à-dire qu'à l'ordinateur, vous faites le calcul. Vous demandez à l'ordinateur de vérifier, de calculer le polynôme minimal, etc. Il vous donne le résultat sans aucune difficulté et il vérifie toutes les propriétés. Et en plus, l'ordinateur va vous donner le groupe de Galois.

Donc, voilà comment le groupe de Galois, comme je vous l'ai dit, il est indexé par des paires de racines de l'équation auxiliaire. Ces paires sont indexées par des entiers et ces entiers sont très spécifiques. Ils sont donnés comme ça, par les racines de l'équation auxiliaire. Et à chaque paire de racines, le groupe de Galois vous donne une permutation. Il vous donne des permutations. Alors là, bien sûr, comme c'est le groupe symétrique, on a toutes les permutations paires possibles entre les racines. Ce n'est pas ce groupe-là en soi qui soit vraiment surprenant. C'est son indexation.

Et ensuite, bien sûr, quand on regarde avec Chebotarev et Dedekind, on s'aperçoit qu'on a effectivement toutes sortes de choses qui peuvent se produire. Vous voyez, par exemple, là, vous avez deux points fixes et puis une permutation cyclique. Là, vous avez un point fixe et deux permutations, deux involutions, etc.

Donc ça, c'est très simple. Alors maintenant, ce que je voulais faire, c'était peut-être aussi... Je n'avais jamais vu faire de manière concrète le fait que quand on adjoint une racine d'une équation auxiliaire, le groupe de Galois, qui était le groupe A_5 ici, va se casser en sous-groupes, mais qui ne seront pas des sous-groupes normaux. Ça, c'est un point essentiel que Galois a compris. Il a compris que quand on adjoint une seule racine d'une équation auxiliaire, le groupe de Galois va diminuer, l'ambiguïté va diminuer, dans des cas particuliers. L'ambiguïté va diminuer, mais elle ne va pas diminuer de manière normale. C'est-à-dire qu'elle va diminuer d'une manière qui dépend du choix de cette racine auxiliaire. C'est extrêmement bizarre. C'est extrêmement bizarre parce que quand vous écrivez la factorisation en polynômes de degrés..., je ne sais plus quels degrés ils ont, ils sont de degré 10, en polynômes de degré 10, quand vous rajoutez cette équation à l'équation de tout à l'heure, à l'équation, je ne l'ai pas choisie au hasard, bien sûr, 109+493x-15x$^2 + 10x^4 + x^6$, quand vous rajoutez cette équation de degré 6, le polynôme se factorise ; il se factorise en termes de la racine adjointe ω. Mais la factorisation ne dépend pas du choix d'ω puisque c'est une factorisation abstraite.

Comment se fait-il que, alors que la factorisation ne dépend pas du choix de ω, le groupe de Galois, lui, se réduise d'une manière qui dépend de ω ? Alors, la manière dont ça arrive, c'est la chose suivante, c'est qu'en fait, ω va prendre six valeurs possibles. Et à chacune de ces six valeurs possibles, quand on regarde les racines d'un terme irréductible du polynôme qui est là, on va obtenir une partition de l'ensemble des 60 racines de l'équation de départ en six sous-ensembles de dix éléments. Alors, j'ai eu beaucoup de mal à la représenter.

J'ai voulu le faire avec des couleurs, ça ne marchait absolument pas, on ne voyait rien. Alors, j'ai finalement opté pour le jeu de cartes et puis j'ai rajouté un loup et puis un symbole un peu connu, c'est celui-là, voilà, d'accord. Et voilà, je vais vous montrer.

Donc, chaque fois que vous rajoutez une racine différente, il y a une partition différente des 60 racines de l'équation auxiliaire. Alors, si je change la racine, ça donne ça. Chaque fois, ce sont des partitions différentes. Chaque fois, ce sont des partitions différentes. Et à chacune de ces partitions, va correspondre un groupe de Galois différent et ce groupe de Galois différent, on peut le calculer, donc. On peut le calculer.

Alors ici, je crois que j'ai calculé pour la partition numéro 3, il me semble. Je vais regarder. Partition numéro 3, c'est ça, d'accord. Donc, je vais simplement vous montrer que ces groupes sont vraiment différents. Alors, il faut que je trouve un élément qui soit un peu typique. Alors, un élément typique, voilà. C'est un élément, par exemple, qui préserve ce point. Alors, je sais que le groupe, ça va être un groupe dihédral d'ordre 10, et je veux distinguer ce sous-groupe du groupe qui correspondra à l'adjonction, je crois que c'est l'adjonction de la numéro 2, ici. Donc, je vais chercher, ah ben voilà, je l'ai.

Ah non, c'est pas possible, ça. Ah non, ces deux-là sont les mêmes, voilà. On va chercher un autre point fixe.

D'accord, donc on va chercher un autre point fixe. Voilà, alors on va prendre ce point fixe-là, d'accord, et je vais le chercher dans le groupe du haut. D'accord, donc je vais chercher dans le groupe du haut, le truc qui fixe le point qui est là.

Alors, je vais chercher. Là, j'ai 10, donc je vais chercher ici. Non, j'ai pas.

Alors, ici. C'est lequel ? C'est celui-là, oui, que je vais fixer. Voilà.

Vous voyez que ce ne sont pas les mêmes. Vous voyez que la permutation qui fixe cette racine, il n'y en aura qu'une, elle n'est pas la même dans le sous-groupe obtenu en adjoignant la racine numéro 3 de la racine numéro 2. D'accord ? Et donc les sous-groupes sont distincts. Bon, alors ça c'était simplement, donc, si vous voulez, une expérimentation, bien entendu. Mais c'est une expérimentation qui, j'espère, montre absolument clairement, je veux dire, l'incroyable vision de Galois qui était capable, sans, à aucun moment, effectuer les calculs, de savoir les résultats que les calculs donneraient, et de voir infiniment plus loin parce que, si vous voulez, non seulement il a été capable de voir qu'une équation primitive est résoluble, si et seulement si on peut indexer ces racines par un corps fini qu'il avait défini et les permutations étant données par le produit semi-direct du groupe affine par le Frobenius, mais en fait il s'est aperçu après qu'il pouvait appliquer sa théorie aux fonctions elliptiques et aux divisions des fonctions elliptiques et c'était pour lui tout à fait un hasard.

Alors je voudrais terminer en revenant sur la fin, si vous voulez, en revenant sur, j'espère que ça va marcher ça, voilà, d'accord, donc en revenant sur la lettre que Galois a écrite à son ami Auguste Chevalier, donc la veille du duel, et dans cette lettre, il dit quelque chose de tout à fait cryptique, impossible presque à comprendre, à quoi on pourrait toujours essayer de donner 36 significations possibles, qui est la chose suivante, c'est dans le paragraphe du milieu :

> "*Tu sais mon cher Auguste que ces sujets ne sont pas les seuls que j'ai explorés, mes principales méditations depuis quelques temps ont été dirigées sur l'application à l'analyse transcendante de la théorie de l'ambiguïté ; il s'agissait de voir, a priori, dans une relation entre des quantités ou fonctions transcendantes quels échanges on pouvait faire* (vous voyez tout à l'heure on a vu pour des équations concrètes algébriques qu'il y a certains échanges qu'on ne pouvait pas faire ; il y a certaines équations qui n'étaient pas possibles comme l'équation $E = 4D^2 + 2D^2$) *quelle quantité on pouvait substituer aux quantités données sans que la relation puisse cesser d'avoir lieu. Cela fait reconnaître tout de suite l'impossibilité de beaucoup d'expressions que l'on pourrait chercher, mais je n'ai pas le temps, et mes idées ne sont pas encore assez développées sur ce terrain qui est immense.*".

Alors, je voudrais conclure si vous voulez de manière à bien faire voir à quel point la pensée de Galois n'est sûrement pas épuisée : la raison c'est la suivante, c'est que maintenant, on a dans les mathématiques modernes, bien sûr, comme je vous l'ai montré, on a parfaitement maîtrisé cette partie qui est la théorie de Galois qui est la théorie des équations etc., on la contrôle infiniment bien. Mais on a un problème analogue, on a un problème analogue plus difficile, bien sûr, que le problème de Galois, et qui est un problème transcendant, et dans ce problème-là, en gros, c'est comme si on avait une équation, ce qu'on appelle les fonctions L, c'est comme si on avait une équation, dont on ne sait même pas démontrer que les racines de cette équation sont toutes réelles ; on ne sait même pas, on en est sûr, parce qu'on peut le vérifier à l'ordinateur, on ne sait même pas démontrer que les racines de cette équation sont toutes réelles. Donc on n'est même pas au premier pas, qui est le pas des physiciens, si vous voulez, qui consiste à regarder où sont les racines de l'équation. Mais le pas suivant, c'est un pas qui est absolument évident tel qu'il est posé par Galois, c'est de développer la théorie de Galois pour ces équations-là. Et ça, ça commence un tout petit peu à exister, mais c'est une théorie qui est bien bien bien loin d'être développée et d'être comprise. Donc il faut bien voir que réduire la théorie de Galois à son application au cadre classique de la théorie des corps, etc., ce serait quelque chose qui serait complètement illusoire parce qu'en fait, dans l'idée fondamentale qui est derrière, l'idée qui est infiniment difficile à expliquer, à saisir, il y a un potentiel qui est beaucoup plus grand que celui qui a été capturé par le formalisme des mathématiques modernes. Voilà je crois que je vais terminer ici.

(Applaudissements)

Le Président de séance : Même ceux qui n'ont pas tout compris, dont je suis, ont été captivés. On vous remercie, beaucoup, et ce qui est intéressant, c'est que vous puissiez dire que tout n'est pas fini, que ça peut encore se développer.

Alain Connes : Bien sûr.

Le Président de séance : La seule question que je voulais vous poser personnellement, c'est de savoir quel crédit on donne à Galois dans les autres pays que notre pays.

Alain Connes : Eh bien en fait, on lui donne plus de crédit qu'en France, puisque par exemple, les corps finis sont appelés les corps de Galois dans tous les pays étrangers. Pas en France ! Donc je vais dire, non, son crédit est immense : je veux dire, ce qu'on appelle groupe de Galois, théorie de Galois, c'est un nom qui est utilisé tout le temps, le nom de Galois est utilisé en permanence ; on appelle extension galoisienne l'extension qui provient de l'équation auxiliaire etc. etc. donc je veux dire il est omniprésent, il est omniprésent. C'est incroyable, cette destinée, c'est une destinée absolument incroyable, penser qu'il n'a jamais eu vraiment la sûreté, à aucun moment, que son travail allait être reconnu, à aucun moment, même au moment où il est mort, je veux dire, à aucun moment, il n'a eu le sentiment que son travail, il faut dire que bon, on comprend, j'espère que vous avez compris, à quel point les relations avec Abel sont complexes et intéressantes, et à quel point, justement, je veux dire, il n'était pas dans une situation simple ; en gros, il a pris le relais, en gros, Abel est mort, et puis Galois est arrivé, il a pris le relais, c'est comme s'ils s'étaient passés le relais de l'un à l'autre, c'est quelque chose d'incroyable. On aurait bien tort de dire "l'un a fait plus que l'autre", ce serait ridicule, ce serait grotesque. Galois avait compris indépendamment, il n'aurait rien fait s'il était parti de là où Abel était, il avait compris indépendamment, il lisait les papiers de Cauchy, les papiers de Lagrange, les papiers de Gauss, et à partir de là, il avait compris énormément de choses...

Le Président de séance : Est-ce que c'est possible d'imaginer ce qu'il aurait fait s'il n'avait pas...

Alain Connes : On n'en sait rien on ne peut absolument rien dire, c'est comme "qu'est-ce que Mozart aurait composé ?". Qui peut dire quoi que ce soit là-dessus personne.

Le Président de séance : Si, Mozart aurait fait de la musique.

Alain Connes : Oui, bon, peut-être.

Le Président de séance : Bien, la discussion est ouverte ; je pense qu'il va y avoir beaucoup de questions.

Jean-Pierre Kahane[2] : Juste où en est-on de la dernière phrase ? C'est-à-dire est-ce qu'on a avancé depuis Galois, sur le programme de Galois, i.e. l'extension aux fonctions transcendantes ?

Alain Connes : Non, il y a pas mal de théories qui peuvent prétendre à ça, en particulier la théorie de Malgrange et Ramis, bien entendu, mais je veux dire, si on est un peu, comment dire, un peu simples, un peu naïfs, on peut dire que ce qui remplace les équations, ce sont les fonctions L. Et on a la notion de factorisation, il y a des fonctions L qui se factorisent etc., il y a des fonctions L dont on pense qu'elles sont irréductibles en un sens convenable etc. La théorie de Galois pour les fonctions L, c'est un peu la théorie des motifs, mais bon, je veux dire, par exemple, trouver des relations non triviales entre les racines, entre les zéros de la fonction ζ de Riemann, pour le moment, personne ne sait rien là-dessus. Donc on voit bien qu'il y a des relations, il y a les fonctions symétriques de la fonction ζ de Riemann, ça, ce sont les formules explicites de Riemann et Weil qui donnent les fonctions symétriques : on les connaît, on les exprime en termes des fonctions qui comptent les nombres premiers, mais les fonctions qui ne sont pas symétriques, est-ce qu'il existe des relations qui ne sont pas des fonctions symétriques, on le sait un peu, parce qu'on a des relations entre les zéros qui imposent de compter les zéros de manière symétrique par rapport à la droite réelle, et ce ne sera pas des relations qui seront invariantes par toutes les symétries, mais on est très peu avancé dans ce domaine et si Galois avait vécu, il aurait peut-être eu l'article de Riemann, sur la conjecture de Riemann, il aurait peut-être développé sa théorie dans ce cadre-là. On n'en sait rien, on ne peut rien dire, personne ne peut dire quoi que ce soit là-dessus.

Le Président de séance : Est-ce qu'il y a d'autres questions ? Monsieur Pecker[3] ?

Jean-Claude Pecker : Excusez-moi, c'est plutôt sur la première partie de ton exposé que je voudrais poser une question : la dernière lettre qui est projetée, celle de Galois à Chevalier, que tu nous as projetée, dit bien qu'il n'a plus eu le temps de faire quelque chose, de développer telle théorie ou telle autre ; est-ce que ça veut dire qu'il s'attendait à être tué en duel ?

Alain Connes : Bon c'est très compliqué, disons qu'il n'a plus eu le temps, c'est plus compliqué que ça. Galois avait passé la dernière année de sa vie en prison. En prison, il a continué à faire des maths et ça, avec un mérite absolument incroyable, parce qu'il n'était pas dans une petite chambre tranquille, avec des bouquins, il était au milieu des autres prisonniers. La prison Sainte-Pélagie, c'était une prison où tous les prisonniers étaient ensemble, et de temps en temps, ses collègues le forçaient à boire. À un moment donné, il avait été obligé de vider une bouteille d'eau de vie, il avait été malade comme un chien, et au moment où Nerval l'a vu dans cette prison, Nerval a dit que Galois avait l'air d'avoir 50 ans ; il n'avait pas encore 20 ans. Donc il était déjà extrêmement usé physiquement, par le fait qu'il continuait à travailler malgré la prison. Alors ensuite ce qui s'est passé, pour le duel, il y a 36 versions, il y a plusieurs versions, il y a la version du bouquin de Infeld, il y a la version du complot, il y a un tas de versions différentes, Jean-Pierre Kahane m'a donné un bouquin qui a une autre version, on ne peut rien dire ; par contre, c'est évident qu'il pensait qu'il n'avait pas beaucoup de chance d'en sortir, de ce duel, il y avait une histoire

[2]Jean-Pierre Kahane, mathématicien français et académicien (1926 - 2017).

[3]Jean-Claude Pecker (1923 - 2020) : astrophysicien français.

de femme, il s'était mis dans de sales draps etc. il avait été provoqué, on ne sait pas, comme je l'ai dit, s'il y avait un complot etc. Mais en tout cas, on imagine mal que Galois était un expert dans le tir au pistolet. Et je ne connais pas les détails, j'avais entendu une fois mais je ne peux pas certifier mes sources, qu'en fait, au lieu d'être un duel dans lequel ils étaient à une vingtaine de mètres et puis ils se rapprochaient à 10 mètres et ils se tiraient l'un sur l'autre, j'ai entendu dire mais je n'en suis pas sûr, qu'en fait, c'était un duel dans lequel un seul des deux pistolets était chargé, ils mettaient chacun le pistolet sur le ventre de l'autre et ils tiraient. Donc bon, je vais dire, il n'a pas eu, il y avait une chance sur deux qu'il s'en sorte, et une chance sur deux qu'il y reste. Et bien sûr, il n'est pas mort tout de suite, il est mort de péritonite, le lendemain, à l'hôpital, vous connaissez l'histoire mais c'est bien évident que quand il disait qu'il n'avait pas le temps, c'est qu'il n'avait pas le temps d'écrire ses idées, mais les idées, il les avait en tête. Quand il disait "je n'ai pas le temps", c'est qu'il n'avait pas le temps d'écrire, mais les idées, il les avait en tête. Ça c'est évident.

Le Président de séance : La chirurgie est honteuse de ne pas avoir pu corriger cette péritonite. Monsieur Balian ?

Roger Balian : C'est simplement pour signaler un tout petit fait, à propos du manque d'hommage officiel à Galois, il y a une rue Galois à Bourg-la-Reine, mais c'est son père.

Alain Connes : C'est son père, absolument, il y a une autre rue Galois à Vitry, mais elle est en dehors du périphérique, et je pense que l'Académie s'honorerait, en demandant qu'une plaque soit mise au 5 rue de la Sorbonne, disant simplement "En cet endroit, Galois a donné un cours d'algèbre en janvier, donc si je me souviens bien, c'est janvier 1830".

Un auditeur : Si vous me permettez, non pas une question, mais deux remarques ; la première, c'est que je crois que le portrait que vous avez montré au début c'est celui de son frère, fait de mémoire par son frère, et non pas par Auguste Chevalier.

Alain Connes : Oui vous avez raison, parfaitement, j'ai hésité, j'avais une hésitation, et c'était une des rares mais celle-là, c'était une hésitation fondée, tout à fait.

Le même auditeur : Alors j'ai une autre remarque c'est qu'il existe une rue Galois dans Paris, mais elle n'est pas à l'intérieur du périphérique, elle est juste à droite de la porte des Lilas, c'est ça elle fait 80 mètres de long, elle n'est effectivement pas à la hauteur du personnage.

Alain Connes : On ne peut pas, c'est insensé, je veux dire...

Le même auditeur : Si vous permettez une troisième chose, c'est que le Conseil de Paris a voté je crois, le 17 octobre, le fait de mettre une plaque à la mémoire d'Évariste Galois au 16 rue des Bernardins, qui est le domicile qu'il avait eu avant sa deuxième incarcération.

Alain Connes : bon bon bon bon bon bon bon.

Le même auditeur : Ça n'interdit absolument pas de mettre une plaque au 5 rue de la Sorbonne.

Alain Connes : Oui pourquoi pas.

Le même auditeur : Il n'y a plus de librairie, mais il y a quand même une grande maison.

Alain Aspect : C'est une blague comme personne n'a de questions sérieuse à poser : on pourrait imaginer un Prix Évariste Galois, et j'étais en train de réfléchir aux sociétés qu'on pourrait solliciter comme sponsor, et il m'est passé par la tête l'idée saugrenue, connaissant la personnalité d'Évariste Galois, qu'on pourrait demander aux banques, qui bénéficient des mathématiques pour faire les choses, je ne suis pas sûr que la mémoire d'Évariste Galois apprécierait, mais par contre, l'idée que vous fassiez quelque chose, les mathématiciens, pour un grand prix Évariste Galois, en trouvant un sponsor honorable, ça peut peut-être se trouver, quand même...

Alain Connes : Oui, mais il y a déjà un prix Abel, je ne sais pas...

Le Président de séance : d'autres questions ? Non... S'il n'y a pas d'autres questions, tout le monde est impressionné, c'est comme cela qu'il faut interpréter ce silence admiratif. On vous remercie infiniment.

(Applaudissements).