CAHIERS DU SÉMINAIRE D'HISTOIRE DES MATHÉMATIQUES

JACQUES DIXMIER

Histoire du 13e problème de Hilbert

Cahiers du séminaire d'histoire des mathématiques 2e série, tome 3 (1993), p. 85-94

<http://www.numdam.org/item?id=CSHM_1993_2_3__85_0>

HISTOIRE DU 13^{e} PROBLEME DE HILBERT

Jacques DIXMIER

Jean-Pierre Kahane a déjà parlé dans ce séminaire du 13^{e} problème de Hilbert ([9a]). Il l'a fort justement appelé "un carrefour de l'algèbre, de l'analyse et de la géométrie". Dans son exposé, il a surtout parlé des aspects analytique et géométrique. Je vais m'intéresser presque exclusivement à l'aspect algébrique.

1. Bring

Les équations générales de degré 2, 3, 4 sont résolues par radicaux dès le XVI^{e} siècle. Au début du XIX^{e} siècle, Abel et Galois prouvent que les équations générales de degré ≥ 5 ne sont pas résolubles par radicaux. Comment surmonter cette impossibilité ?

Pour décrire une des voies possibles, il faut remonter en 1786. Cette année-là paraît à Lund la thèse de E.S. Bring ([3]). (Je n'ai pu consulter la thèse, mais le passage relatif à l'équation du 5^{e} degré est reproduit à la fin de [6]). Bring prouve que, après résolution d'équations auxiliaires de degrés 2 et 3, l'équation générale du 5^{e} degré se ramène à la forme $x^5 + x = a$, donc peut se résoudre à condition d'admettre une fonction algébrique spéciale d'une seule variable $x = f(a)$. Or les radicaux, eux aussi, sont des fonctions algébriques d'une seule variable. D'où le problème un peu vague : quelles équations algébriques peut-on résoudre en superposant des fonctions algébriques d'une seule variable et des fonctions rationnelles ?

Observons que toute fonction rationnelle s'obtient en superposant des fonctions d'un variable et la seule fonction de deux variables $x+y$; en effet,

$$x - y = x + (-y)\ ,\ \ xy = \frac{1}{4}[(x + y)^2 - (x-y)^2)]\ ,\ \frac{x}{y} = x \cdot \frac{1}{y}$$

(nous ne considérerons que des corps de caractéristique 0).

2. Quelques définitions

Pour faciliter l'exposé, donnons tout de suite des définitions modernes et précises.

Soit k un corps de base (commutatif) fixé une fois pour toutes. Les définitions qui suivent dépendent de k.

Soient K une extension de k, r un entier > 0.
Une extension L de K est dite r-élémentaire s'il existe $x_1, \ldots\ldots, x_r \in K$, et une extension de degré fini H de $k(x_1, \ldots\ldots, x_r)$ tels que L soit engendrée par H et K.

Une extension L de K est dite *de niveau* $\leq r$ s'il existe une chaîne d'extensions :

$$K = K_0 \subset K_1 \subset K_2 \subset \ldots\ldots \subset K_n$$

telle que : 1) $K \subset L \subset K_n$;

2) pour $i = 1, 2, \ldots\ldots, n$, K_i est une extension r-élémentaire de K_{i-1}.

(Il est clair qu'alors L est de degré fini sur K).

Une extension L de K est dite de niveau r si elle est de niveau ≤ r, mais pas de niveau ≤ r - 1.

Des définitions équivalentes ont été données par V. Arnold et G. Shimura ([1], p. 45-46).

Dans la suite, on prendra $k = \mathbb{C}$, mais cela n'a pas beaucoup d'importance.

Soient $A_0, A_1, \ldots\ldots, A_{n-1}$ des indéterminées, K le corps $k(A_0, A_1, \ldots\ldots, A_{n-1})$, L le corps des racines de l'équation générale du n-ième degré $X^n + A_{n-1} X^{n-1} + A_{n-2} X^{n-2} + \ldots + A_0 = 0$. *Soit s(n) le niveau de l'extension L de K.*

Le 13^e problème de Hilbert peut être provisoirement présenté comme le calcul de s(n) (on reviendra là-dessus). Dire que $s(n) \leq 4$ par exemple pour un certain n signifie intuitivement que l'équation générale de degré n peut se résoudre en superposant des fonctions algébriques d'au plus 4 variables.

3. Jerrard

En 1786, on savait donc que

$$s(2) = s(3) = s(4) = s(5) = 1.$$

Mais la thèse de Bring passa inaperçue et ne fut exhumée qu'en 1861 par C. Hill (*cf.* [6]). Dans l'intervalle, le résultat fut retrouvé par G.B. Jerrard ([9]). La méthode de Jerrard, comme celle de Bring, consiste à faire des transformations de Tschirnhaus bien choisies. Mais Jerrard, qui appliquait d'ailleurs aussi sa méthode à des équations de degré > 5, commet des erreurs graves. En particulier, il prétend résoudre par radicaux l'équation du 5^e degré !

4. Hamilton

W. Hamilton, qui connaissait le résultat d'Abel (il a même écrit un mémoire pour éclaircir des points douteux de la preuve d'Abel) a immédiatement rédigé un long article [4] dans lequel, entre autres choses, il dissèque soigneusement l'erreur de Jerrard. (Cela n'a pas empêché Jerrard de continuer, pendant des années, à proclamer par écrit la validité de sa méthode).

Ouvrons ici une parenthèse. Dans [4], Hamilton observe que, par une variante de la méthode de Jerrard, il n'est pas loin de ramener l'équation générale du 6^e degré à la résolution d'équations auxiliaires de degrés ≤ 5. Bien qu'il n'y réussisse pas, l'espoir, pour lui, subsiste. Autrement dit, s'il connaît Abel, il n'a pas entendu parler, en 1837, de Galois. (Rappelons que les oeuvres de Galois n'ont été publiées qu'en 1846).

Revenons à [4]. Hamilton vérifie soigneusement que Jerrard, malgré ses erreurs, a effectivement ramené l'équation générale du 5^e degré à la forme $x^5 + x = a$. Dans [5], Hamilton mentionne qu'il a construit des tables numériques exploitant cette réduction pour résoudre les équations du 5^e degré - ce qui fera sourire, je suppose, les analystes numériciens modernes.

Hamilton observe que la méthode de Jerrard permet, pratiquement sans changement, de faire disparaître les termes de degrés $n-1, n-2, n-3$ dans l'équation générale du n-ième degré, pour $n \geq 5$; ce qui entraîne aussitôt $s(n) \leq n-4$ pour $n \geq 5$; par exemple

$$s(6) \leq 2 \ , \ s(7) \leq 3 \ , \ s(8) \leq 4 \ , \ s(9) \leq 5 \ , \ s(10) \leq 6 \ .$$

Mais il va plus loin et prouve, en raffinant la méthode de Jerrard, que :

(*) On peut faire disparaître les termes de degrés $n-1, n-2, \ldots, n-i$ sans avoir à résoudre d'équation de degré $> i$, et ceci pourvu que n majore un certain entier H_i ;

et Hamilton trouve :

$$H_3 = 5 \ , \ H_4 = 11 \ , \ H_5 = 47 \ , \ H_6 = 923 \ .$$

Les entiers H_i ont été appelés "nombres de Hamilton" par Sylvester.

Ce qui précède entraîne aussitôt

$$\begin{array}{lll} s(n) \leq n-5 & \text{pour} & n \geq 11 \\ s(n) \leq n-6 & \text{pour} & n \geq 47 \\ s(n) \leq n-7 & \text{pour} & n \geq 923. \end{array}$$

La méthode conduit au problème suivant : étant donnée une variété algébrique projective Σ définie par des équations homogènes

$$\varphi_1 (x_1 ,\ldots, x_m) = \varphi_2 (x_1 ,\ldots, x_m) = \ldots = \varphi_p (x_1 ,\ldots, x_m) = 0$$

de degrés $\leq d$ à coefficients dans K, trouver un point de Σ dont les coordonnées sont algébriques de degré $\leq d$ sur K. Le problème est explicitement posé par Jerrard (appelons-le "problème de Jerrard" dans la suite). Hamilton prouve que, lorsque p et les degrés des φ_i sont fixés, le problème de Jerrard admet une solution, pourvu que $m \geq m_o$, et il donne un algorithme pour calculer un m_o (pas le meilleur possible).

5. Sylvester

J.J. Sylvester, dans [16], a repris et un peu amélioré la méthode de Hamilton. Il retrouve l'énoncé (*), mais avec des entiers $H'_i < H_i$:

$$H'_4 = 10 \ , \ H'_5 = 44 \ , \ H'_6 = 905 \ , \ldots$$

(en fait, l'amélioration $H_4 \rightarrow H'_4$ avait déjà été observée par Hamilton).

D'où des majorations améliorées des s(n), par exemple

$$s(10) \leq 5 .$$

Toutefois, J. Hammond et Sylvester prouvent dans [17] que $H_{i+1} \sim \frac{1}{2} H_i^2$ quand $i \to \infty$, et de même pour les H'_i, de sorte que ces nombres croissent beaucoup plus vite que i!. Les majorations obtenues pour les s(n) sont donc rapidement illusoires. Par exemple, dans l'équation générale de degré n, on peut faire disparaître les termes de degrés n-1 , n-2 ,..., n-6 sans avoir à résoudre d'équation de degré ≥ 720. D'où $s(n) \leq n-7$ pour $n \geq 727$, résultat d'ailleurs facile à améliorer.

Sylvester utilise un peu le langage de la géométrie à n dimensions, alors que le langage de Hamilton restait purement algébrique.

Les mémoires de Hamilton et Sylvester ont été oubliés par la suite. Par exemple, Klein, Hilbert, Wiman, Brauer, Segre, dans des mémoires dont nous allons parler, ne les citent pas (ils mentionnent par contre Bring et Jerrard).

6. Klein

De 1877 à 1905, plusieurs mémoires de F. Klein (*cf.* par exemple [10], [11], [12]) tournent autour des mêmes questions pour les équations de degrés 5, 6, 7, 8. Pour commencer, Klein ramène l'équation générale du 5^e degré à la résolution d'une équation en z :

$$F(z,a) = 0 \qquad (**)$$

contenant un seul paramètre a (F est un polynôme). Il retrouve donc que s(5) = 1.

L'équation (**) est de degré 60 en z ! Le résultat semble donc infiniment moins bon que celui de Bring. Toutefois, cette équation (**), dite équation icosaédrale, est liée à une foule de questions intéressantes.

Le point essentiel pour Klein est que le groupe de Galois de l'équation générale du 5^e degré, c'est-à-dire le groupe alterné A_5 (on suppose adjointe la racine carrée du discriminant) admet une représentation projective de dimension 1. (En effet, A_5 admet pour revêtement d'ordre 2 le groupe icosaédral binaire, lequel admet une représentation linéaire évidente de dimension 2).

Pour les équations de degrés 6, 7, 8, Klein utilise de même des représentations projectives de petites dimensions des groupes A_6, A_7, A_8. Toutefois, il n'obtient même pas la majoration $s(6) \leq 2$ de Hamilton; il lui faut pour cela attendre que Valentiner, en 1889, découvre une représentation projective de dimension 2 de A_6.

7. Hilbert

Dans sa liste de problèmes au Congrès de Paris en 1900, Hilbert pose son "13^e problème" ([7]). Pour fixer les idées, il se concentre sur le cas des équations de degré 7. Mais, brusquement, le problème change de nature. Car voici comment Hilbert formule son problème :

L'équation du septième degré $f^7 + x f^3 + y f^2 + z f + 1 = 0$ est impossible à résoudre au moyen de fonctions continues quelconques de deux arguments seulement. (Il s'agit certainement d'un problème local).

Hilbert parle donc de *fonctions continues*, alors que toute la tradition du XIXe siècle aurait dû l'inciter à parler de fonctions algébriques. En outre, dans les généralités qui entourent le problème, Hilbert fait allusion à la nomographie. En 1976, V. Arnold et G. Shimura ([1]) se sont demandés pourquoi Hilbert avait formulé son problème en termes de fonctions continues; sans doute, suggèrent-ils, Hilbert espérait une preuve d'impossibilité même dans le cadre des fonctions continues. En fait, Arnold et Kolmogorov ont prouvé en 1957 que toute fonction continue de n variables s'obtient en superposant des fonctions continues d'une variable; ce qui tue le problème de Hilbert. C'est d'ailleurs le début d'une histoire intéressante, mais nous n'en parlerons pas (*cf.* par exemple [13], ou bien l'exposé de J.-P. Kahane [9a] déjà cité).

Nous retiendrons le 13e problème de Hilbert sous sa forme algébrique. C'est sous cette forme qu'il est présenté par Arnold et Shimura (pour les équations de degré n).

Hilbert est revenu en 1927 sur son 13e problème, dans un de ses derniers mémoires ([8]). Et là, il donne les *deux* aspects du problème ("continu" et "algébrique"). Il conjecture que

$$s(6) = 2,\ s(7) = 3\ \ (13^e \text{ problème}),\ s(8) = 4,$$

et il prouve que

$$s(n) \leq n - 5 \text{ pour } n \geq 9 \text{ (en particulier, } s(9) \leq 4).$$

Ce résultat est réétabli presque aussitôt par Wiman ([19]); sa méthode est plus simple.

8. Après Hilbert

L'histoire est presque terminée. N. Tschebotaröw annonce des travaux sur le sujet dans deux mémoires ([18]), mais n'a rien publié. Brauer ([2]) et Segre ([14], [15]) posent explicitement le problème de Jerrard, mais vont moins loin que Hamilton et Sylvester à certains égards; par exemple, Segre énonce seulement que $s(n) \leq n - 6$ pour $n \geq 157$. Segre retrouve la méthode de Wiman (apparemment, il n'a pas connaissance de [19]). A mon sens, les démonstrations par Hilbert et Wiman que $s(9) \leq 4$ ne sont pas tout à fait complètes. (Ils traitent certaines formes comme des formes génériques, alors qu'elles ne le sont pas). Segre est plus sérieux, mais passe sur certains détails. Comme toute l'affaire est finalement très simple, je donne une preuve que j'espère complète, adaptée de Wiman, en appendice.

Comme on l'a dit, Arnold et Shimura rappellent l'aspect algébrique du 13e problème.

C'est tout, à ma connaissance.

Terminons sur une note dramatique, qui prouve notre incroyable ignorance. Bien que cela paraisse improbable, il n'est pas exclu que $s(n) = 1$ pour tout n ! Autrement dit, le théorème d'Arnold-Kolmogorov pourrait être vrai dans le cadre algébrique. Toute *minoration* de $s(n)$ serait un progrès sérieux. En particulier, il serait temps de savoir si $s(6) = 1$ ou $s(6) = 2$.

Bibliographie

[1] V. Arnold et G. Shimura, *Proc. Symposia in pure math.*, 28 (1976), AMS, Providence, p. 45-46.

[2] R. Brauer, A note on systems of homogeneous algebraic equations, *Bull. Amer. Math. Soc.*, 51 (1945), p. 749-755.

[3] E.S. Bring, *Meletemata quaedam mathematica circa transformationem aequationum algebraicarum*, Univ. de Lund, 1786.

[4] W. Hamilton, Inquiry into the validity of a method recently proposed by George B. Jerrard, Esq., for transforming and resolving equations of elevated degree, *Bristish Assoc. Report*, 1837, p. 295-348.

[5] W. Hamilton, Investigations respecting equations of the fifth degree, *Proc. Roy. Irish Acad.*, 1 (1841), p. 76-80.

[6] R. Harley, A contribution to the history of the problem of the reduction of the general equation of the fifth degree to a trinomial form, *Quarterly J. Math.*, 6 (1864), p. 38-47.

[7] D. Hilbert, Sur les problèmes futurs des Mathématiques, *Compte rendu du deuxième Congrès international des mathématiciens (1900)*, Paris, Gauthier-Villars, 1902, p. 58-114.

[8] D. Hilbert, Über die Gleichung neunten Grades, *Math. Ann.*, 97 (1927), p. 243-250.

[9] G.B. Jerrard, *Mathematical Researches*, Longman, Bristol and London, 1834.

[9a] J.-P. Kahane, Le 13^{e} problème de Hilbert : un carrefour de l'algèbre, de l'analyse et de la géométrie, *Cahiers du Séminaire d'Histoire des Mathématiques*, (1re série) 3 (1982), p. 1-22.

[10] F. Klein, Über die Auflösung gewisser Gleichungen vom siebenten und achten Grade, *Math. Ann.*, 15 (1879), p. 251-282.

[11] F. Klein, Zur Theorie der allgemeinen Gleichungen sechsten und siebenten Grades, *Math. Ann.*, 28 (1886), p. 499-532.

[12] F. Klein, Über die Auflösung der allgemeinen Gleichungen fünften und sechsten Grades, *Math. Ann.*, 61 (1905), p. 50-71.

[13] G.G. Lorentz, The 13-th problem of Hilbert, *Proc. Symposia in pure math.*, 28 (1976), AMS, Providence, p. 419-430.

[14] B. Segre, The algebraic equations of degrees 5, 9, 157,..., and the arithmetic upon an algebraic variety, *Ann. of Math.*, 46 (1945), p. 287-301.

[15] B. Segre, *Arithmetical questions on algebraic varieties*, Athlom Press, London, 1951.

[16] J.J. Sylvester, On the so-called Tschirnhausen Transformation, *J. für die reine und angewandte Math.,* 100 (1887), p. 465-486.

[17] J.J. Sylvester et J. Hammond, On Hamilton's numbers, *Phil. Trans. Royal Soc. of London*, 178 (1887), p. 285-312; et 179 (1888), p. 65-71.

[18] N. Tschebotaröw, Über ein algebraisches Problem von Herrn Hilbert, I-II, *Math. Ann.*, 104 (1931), p. 459-471; et 105 (1931), p. 240-255.

[19] A. Wiman, Über die Anwendung der Tschirnhausen-Transformation auf die Reduktion algebraischer Gleichungen, *Nova acta regiae societatis scientiarum Uppsaliensis*, 16 (1927), p. 3-8.

APPENDICE

1. Soient K un corps commutatif, E un espace vectoriel de dimension finie sur K, K' une extension de K, $E' = E \otimes_K K'$. Si $\varphi : E \to K$ est une forme de degré n sur E, on notera encore φ l'unique forme de degré n sur E' qui prolonge φ.

2. Lemme : *Soient $q : K^5 \to K$ et $q' : K^5 \to K$ des formes quadratiques sur K^5, $r : K^5 \to K$ une forme cubique sur K^5. Il existe :*

une extension K' de K de niveau ≤ 2

un $x \in K'^5 \setminus \{0\}$

tels que $q(x) = q'(x) = r(x) = 0$.

Il existe dans une clôture algébrique de K un élément λ de degré ≤ 5 sur K tel que $q + \lambda q'$ ou $q' + \lambda q$ (disons $q' + \lambda q$ par exemple) soit dégénérée. Comme $s(5) = 1$, il existe une extension K_1 de niveau 1 de K telle que $\lambda \in K_1$.

Il existe une extension K_2 de K_1, déduite de K_1 par une succession d'extensions quadratiques, avec la propriété suivante : par rapport à une base convenable $(e_1, \dots, e_5)$ de $(K_2)^5$, on a :

$$(q' + \lambda q)(z_1 e_1 + \dots + z_5 e_5) = z_1 z_2 + z_3 z_4.$$

Posons :

$$E = K_2 e_1 + K_2 e_3 + K_2 e_5 .$$

Il existe une extension K' de K_2, obtenue en adjoignant à K_2 les racines d'équations de degrés ≤ 6, telle que les équations

$$x \in E \otimes_{K_2} K', \; q(x) = r(x) = 0$$

aient une solution non nulle. Comme $s(6) \leq 2$, K' est une extension de niveau ≤ 2 de K_2 donc de K.

Comme $x \in E \otimes_{K_2} K'$, on a $(q' + \lambda q)(x) = 0$. Comme $q(x) = 0$, on a $q'(x) = 0$.

3. Lemme :*Soient $q : K^8 \to K$, $r : K^8 \to K$, $s : K^8 \to K$ des formes de degrés 2, 3, 4 sur K^8. Il existe :*

une extension K' de K de niveau ≤ 2

un $x \in K'^8 \setminus \{0\}$

tels que $q(x) = r(x) = s(x) = 0$.

En remplaçant K par une extension de niveau ≤ 2, on se ramène d'abord au cas où il existe $x_0 \in K^8 \setminus \{0\}$ tel que $q(x_0) = r(x_0) = 0$. Choisissons un supplémentaire S de Kx_0 dans K^8.

Pour $\lambda \in K$ et $y \in S$, on a

$$q(\lambda x_0 + y) = \lambda\varphi_1(y) + \varphi_2(y)$$
$$r(\lambda x_0 + y) = \lambda^2\psi_1(y) + \lambda\psi_2(y) + \lambda\psi_3(y)$$

où φ_i, ψ_i sont des formes de degré i sur S à valeurs dans K.

Soit T un sous-espace vectoriel de dimension 5 de S contenu dans $\mathrm{Ker}\varphi_1 \cap \mathrm{Ker}\psi_1$. Appliquons le lemme 2 aux restrictions $\varphi_2|T$, $\psi_2|T$, $\psi_3|T$. On obtient une extension K_1 de K de niveau ≤ 2, et un $y_0 \in T_1 \setminus \{0\}$ (où l'on pose $T_1 = T \otimes_K K_1$) tels que

$$\varphi_2(y_0) = \psi_2(y_0) = \psi_3(y_0) = 0.$$

Alors $q(\lambda x_0 + \mu\, y_0) = r(\lambda x_0 + \mu y_0) = 0$ quels que soient λ et μ dans K_1. Il existe une extension K' de K_1, de degré ≤ 4, et un élément non nul x de $K'x_0 + K'y_0$, tels que $s(x) = 0$. On a $q(x) = r(x) = 0$. Et K' est une extension de K de niveau ≤ 2.

4. <u>Théorème</u> : *On a $s(n) \leq n\text{-}5$ pour $n \geq 9$.*

Soient $u_0, u_1, \ldots, u_{n-1} \in K$, et x une racine de l'équation

(1) $$x^n + u_{n-1}x^{n-1} + u_{n-2}\, x^{n-2} + \ldots + u_0 = 0$$

Faisons une transformation de Tschirnhaus

(2) $$y = \alpha_0 + \alpha_1 x + \alpha_2\, x^2 + \ldots + \alpha_{n-1}\, x^{n-1}$$

$(\alpha_0, \ldots, \alpha_{n-1} \in K)$. L'équation en y, obtenue en prenant le résultant de (1) et (2), est de la forme

(3) $$y^n + C_1(\alpha_0,\ldots, \alpha_{n-1})\, y^{n-1} + C_2(\alpha_0,\ldots, \alpha_{n-1})\, y^{n-2} + \ldots + C_n(\alpha_0,\ldots, \alpha_{n-1}) = 0$$

où $C_i(\alpha_0,\ldots, \alpha_{n-1})$ est une forme de degré i à coefficients dans K.

Le coefficient de α_0 dans $C_1(\alpha_0,\ldots, \alpha_{n-1})$ est n. Tirons α_0 en fonction de $\alpha_1,\ldots, \alpha_{n-1}$ de l'équation $C_1 = 0$, et portons dans les C_i ; alors C_i devient une forme D_i de degré i en $\alpha_1,\ldots, \alpha_{n-1}$. Comme $n-1 \geq 8$, il existe (lemme 3) une extension K_1 de K de niveau ≤ 2, et $\alpha_1,\ldots, \alpha_{n-1}$ non tous nuls, tels que

$$D_2(\alpha_1,\ldots, \alpha_{n-1}) = D_3(\alpha_1,\ldots, \alpha_{n-1}) = D_4(\alpha_1,\ldots, \alpha_{n-1}) = 0.$$

Faisons désormais un tel choix de $\alpha_1,\ldots, \alpha_{n-1}$, d'où une valeur de α_0. Alors les termes en y^{n-1}, y^{n-2}, y^{n-3}, y^{n-4} ont disparu de (3). Par adjonction à K_1 d'un radical, on peut en outre supposer $C_5(\alpha_0,\ldots, \alpha_{n-1}) = 0$ ou 1. Il existe donc une extension K_2 de niveau $\leq n\text{-}5$ de K_1

qui contient y. Or (2) est une équation en x de degré $\leq$ n-1 à coefficients dans K_2. Par récurrence sur n, il existe une extension K' de K_2 de niveau $\leq$ n-5 qui contient x.

(*texte reçu le 13 novembre 1991*)