Histoire des équations algébriques

Arnaud Beauville

Introduction

Ce texte est une partie (= 8 heures de cours) du cours d'histoire des Mathématiques en 3$^{\text{ème}}$ année de Licence. Il essaie de retracer l'histoire des équations algébriques depuis les débuts de l'écriture jusqu'à son point actuel – atteint essentiellement au 19$^{\text{ème}}$ siècle.

Je n'ai évoqué que brièvement l'apparition de l'équation du second degré, qui relève plus de l'histoire que des mathématiques. Les choses sérieuses commencent avec la Renaissance italienne et l'histoire mouvementée de la résolution de l'équation du 3$^{\text{ème}}$ degré. Après ce feu d'artifice se place une période de consolidation: les idées se clarifient, la notation algébrique utilisée de nos jours s'impose peu à peu, de nouvelles attaques se développent. Puis vient l'âge d'or, où les travaux de trois grands mathématiciens, Lagrange, Abel et Galois, conduisent à une compréhension complète de l'ensemble du problème.

Plan

Références

Il faut avant tout recommander le site "MacTutor" de l'Université de Saint Andrews: `http://www-history.mcs.st-andrews.ac.uk/history/`
qui contient des milliers de biographies de mathématiciens ainsi que des fiches historiques sur les principaux développements mathématiques. Je m'en suis largement inspiré dans ce texte.

Le livre de J.-P. Tignol, "Galois theory of Algebraic Equations" (World Scientific) est un bon mélange d'histoire et de mathématiques – celles-ci à un niveau un peu supérieur à celui de la licence.

CHAPITRE I

Préhistoire: l'équation du second degré

1. L'antiquité

Le premier témoignage connu de résolution d'une équation du second degré se trouve sur une tablette babylonienne, datant environ de 2000 avant J.-C.:

« J'ai soustrait le côté de mon carré de son aire: 870. Prenez 1, le coefficient. Divisez 1 en 2 parties: 0,5. Multipliez 0,5 par lui-même: 0,25. Ajoutez à 870: 870,25 qui a la racine 29,5. Ajoutez à 29,5 le 0,5 que vous avez multiplié par lui-même: 30, c'est le côté du carré. »

En termes modernes: "la" solution de $x^2 - x = 870$ est égale $\frac{1}{2} + \sqrt{(\frac{1}{2})^2 + 870} = 30$.
Quelques remarques:

– en fait les babyloniens comptaient en base 60.

– Le problèème est de nature arithmétique: géométriquement soustraire une longueur d'une aire n'a pas de sens.

– "La" solution est la solution *positive*: les nombres négatifs sont inconnus. Ce problèème va handicaper le développement de l'algèbre jusqu'au $17^{\text{ème}}$ siècle. Par exemple, il faut distinguer trois types d'équations du second degré:

$$x^2 + px = q \quad , \quad x^2 = px + q \quad , \quad x^2 + q = px \ .$$

Chacun de ces types d'équations est considéré dans les textes babyloniens; bien entendu, avec des exemples numériques, et sous forme de problèmes concrets comme ci-dessus – la notation algébrique moderne n'est apparue qu'au 17ème siècle.

– La notion de nombre irrationnel est aussi absente. La plupart des problèmes sont posés de façon à admettre une solution entière. Quand ce n'est pas le cas, on approxime: on trouve ainsi dans une tablette babylonienne une approximation de $\sqrt{2}$ correcte à 10^{-5} près.

Les Grecs, au contraire, découvrent l'existence des nombres irrationnels, en particulier celle de $\sqrt{2}$ (école de Pythagore, $5^{\text{ème}}$ siècle avant J.-C.). Si l'on en croit Aristote, la démonstration était celle que l'on utilise encore maintenant (si $\sqrt{2} = \frac{p}{q}$, $p^2 = 2q^2$, d'où p pair, puis q pair). Cette découverte semble avoir produit une grande méfiance vis-à-vis de la notion de nombre, et explique sans doute en partie que les mathématiques grecques soient centrées sur la géométrie: les problèmes algébriques sont ramenés à des problèmes géométriques, le plus souvent l'intersection de 2 courbes simples (droites, coniques...). La géométrie fait du même coup des progrès considérables, qui culminent avec les *Éléments* d'Euclide[1] (~ 280 avant J.-C.). Certains résultats sont très proches de la résolution d'une équation du second degré (cf. Proposition 5 du Livre II), mais ils sont toujours énoncés géométriquement.

[1] On sait très peu de choses sur la vie d'Euclide d'Alexandrie – son existence même comme individu est parfois contestée.

2. Les mathématiques indiennes et arabes

Chronologiquement ce sont les mathématiciens indiens qui prennent le relais. Brahmagupta (598-670) écrit deux traités de mathématiques et astronomie, l'un en 628 et l'autre en 665. Il introduit le zéro et les nombres négatifs, la règle des signes (en termes de "fortune" et de "dette" : le produit de deux dettes est une fortune, etc.).

Bien que les mathématiciens arabes aient connu ces travaux, ils n'ont pas fait usage des nouveautés introduites par Brahmagupta. Le plus célèbre est al-Khwarizmi (environ 780-850, Bagdad), qui est (indirectement) responsable des mots *algorithme* (tiré de son nom) et *algèbre*: "al-jabr" (qui signifie à peu près "restauration") est, avec "al-muqabala" une des deux opérations de base qui lui permettent de traiter les équations algébriques; *al-jabr* permet de passer par exemple de $x^2 = 40x - 4x^2$ à $5x^2 = 40x$ (en écriture moderne! la notation algébrique est encore inexistante).

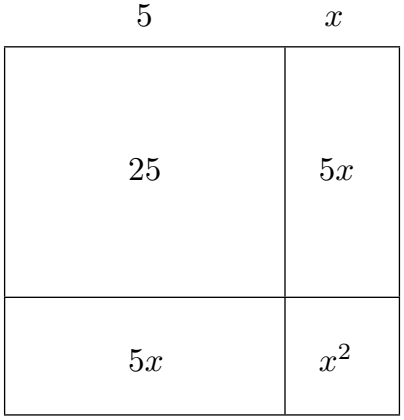
Al-Khwarizmi fait une étude systématique des équations du $2^{\text{ème}}$ degré. Il distingue 6 types:

1. Carré égal à la racine (en langage moderne, $x^2 = 7x$ par exemple)
2. Carré égal à un nombre.
3. Racine égale à un nombre.
4. Carré plus racine égal à un nombre, par exemple $x^2 + 10x = 39$.
5. Carré plus nombre égal à la racine: $x^2 + 21 = 10x$.
6. Racine plus nombre égal au carré: $3x + 4 = x^2$.

Il donne dans chaque cas, sur un exemple, la recette algébrique pour trouver la solution. Par exemple, pour l'équation $x^2 + 10x = 39$:

« ... la manière de résoudre ce type d'équation est de prendre la moitié des racines [= du coefficient de x], dans notre cas, 10. Donc prenez 5, qui multiplié par lui-même donne 25, que vous ajoutez à 39 ce qui donne 64. Ayant pris la racine carrée de ce nombre qui est 8, soustrayez-en la moitié des racines 5 ce qui laisse 3. Ainsi 3 est la racine du carré, qui lui-même est donc 9. »

La recette étant donnée, Al-Khwarizmi en donne une démonstration géométrique, par ce qu'on appelle la "complétion du carré": le carré de côté $x + 5$ a pour aire $39 + 25 = 64$, donc $x + 5 = 8$.



Omar KHAYYAM (1048-1131), Persan, est surtout connu comme poète pour ses quatrains (*Rubaiyat*). Comme beaucoup de mathématiciens de l'époque, il était aussi astronome. En algèbre il a commence l'étude des équations du 3ème degré, qu'il résoud graphiquement: par exemple le point d'intersection de la parabole $y = \frac{x^2}{a}$ avec le cercle de centre $(\frac{c}{2}, 0)$ passant par O a pour abscisse x solution de $x^3 + a^2x = ca^2$.

Il discute ainsi les 6 types d'équations du 3ème degré à 3 termes:

$$x^3 + px = q \quad , \quad x^3 + q = px \quad , \quad x^3 = px + q \quad ,$$

et la même chose en remplaçant x par x^2 . Dans chaque cas il indique une solution géométrique. Il discute ensuite les équations avec 4 termes.

CHAPITRE II

La Renaissance italienne

3. L'équation du 3ème degré

La seconde moitié du 15ème siècle est en Italie une période d'effervescence intellectuelle, artistique et scientifique. La découverte de la perspective et sa codification (Piero della Francesca, Léonard de Vinci) créent le besoin d'une base mathématique solide. En 1494, Luca Pacioli publie la *Summa de arithmetica, geometria, proportioni et proportionalita*, somme des connaissances de l'époque, un des premiers livres de mathématiques imprimé. Il traite surtout l'équation du second degré, mais discute à la fin les équations de degré plus grand et déclare que leur résolution est "impossible dans l'état actuel de la science".

Il est admis à ce point que le problème majeur est celui de l'équation du 3ème degré "nombre, chose et cube", c'est-à-dire sans terme en x^2 (la "chose", *cosa* en italien, désigne l'inconnue). On sait maintenant que toute équation de degré 3 se

ramène à ce cas en faisant une translation sur la variable, mais ce procédé, qui peut transformer une racine positive en racine négative, n'est pas utilisé à l'époque. Compte tenu des signes des coefficients, il y a donc 3 cas:

$$x^3 + px = q \quad , \quad x^3 = px + q \quad , \quad x^3 + q = px \quad .$$

Il est utile d'observer que les deux premiers cas ont exactement une solution positive, tandis que le dernier en a 2 ou 0 .

Scipione DEL FERRO (1465-1526, professeur à l'Université de Bologne) résoud le premier cas vers 1515 mais garde le résultat secret jusque peu avant sa mort, en 1526, où il révèle sa méthode à son élève Antonio FIOR.

Fior était semble-t-il un mathématicien plutôt médiocre, et il commença à se vanter d'avoir résolu l'équation du $3^{\text{ème}}$ degré. En 1535 est organisée une compétition entre lui et Tartaglia[2] : chacun propose à l'autre 30 problèmes. Fior donne tous ses problèmes sous la forme du premier type, résolue par del Ferro. Mais quelques jours avant Tartaglia avait découvert la solution de tous les cas, et résoud les 30 problèmes en moins de 2 heures, tandis que Fior fait médiocre figure.

Entre en scène Girolamo CARDANO – Cardan en français (1501–1576). Fils illégitime d'un avocat mathématicien amateur, il fait des études de médecine à Milan. Il obtient son doctorat de médecine en 1525, mais sa candidature est rejetée par le Conseil des médecins de Milan – sans doute à cause de sa franchise souvent agressive, de sa naissance illégitime, et aussi de sa passion du jeu qui l'amène à des fréquentations peu recommandables. Il se trouve vite au bord de la misère, mais obtient heureusement un poste d'enseignant à la Fondation Piatti de Milan. Il y exerce à la fois la médecine et les mathématiques, et commence à publier des articles ou des livres dans divers domaines – mathématiques, médecine, astronomie, philosophie...

Cardan explique qu'il avait pris au pied de la lettre l'affirmation de Pacioli suivant laquelle il était impossible de résoudre l'équation du $3^{\text{ème}}$ degré; il est donc très étonné par l'annonce de cette résolution, et il demande à Tartaglia de lui expliquer sa méthode. Tartaglia commence par refuser. Cardan lui fait miroiter ses relations haut placées, en particulier le gouverneur de Milan, qui pourraient favoriser sa carrière. En 1539 Tartaglia accepte de faire le voyage de Venise à Milan; là il se laisse convaincre, en faisant jurer à Cardan de ne jamais divulguer la solution, qu'il écrit sous forme de poème:

[2] Nicolo de Brescia (1499–1557), dit TARTAGLIA ("le bègue"), avait eu une partie du visage détruit à 13 ans lors du sac de Brescia, sa ville natale, par les Français – ce qui explique son surnom ainsi que la superbe barbe qu'il porte sur tous ses portraits. Autodidacte, il enseigne au niveau secondaire à Vérone puis Venise, mais acquiert peu à peu une solide réputation de mathématicien.

Quando chel cubo con le cose appresso se agguaglia à qualche numero discreto trovan dui altri differenti in esso. Dapoi terrai questo per consueto Che'l lor produtto sempre sia eguale Al terzo cubo delle cose neto, El residuo poi suo generale Delli lor lati cubi ben sottratti Varra la tua cosa principale...	Quand le cube et la chose ensemble sont égaux à un nombre donné Trouvez deux autres nombres qui diffèrent de celui-ci. De plus prenez pour habitude Que leur produit soit toujours égal Au cube tiers de la chose. Le résultat, de manière générale, de la soustraction de leurs racines cubiques Sera égal à la chose principale.

En termes modernes: on cherche la solution de $x^3 + px = q$ sous la forme $x = u - v$. Compte tenu de l'identité

$$(u - v)^3 = u^3 - v^3 - 3uv(u - v) \ ,$$

on a
$$x^3 + px = u^3 - v^3 + (u - v)(-3uv + p) \ ,$$

donc l'équation est satisfaite si $3uv = p$ et $u^3 - v^3 = q$. Autrement dit,
$u^3 v^3 = \left(\frac{p}{3}\right)^3$ ("leur produit est égal au cube tiers de la chose.")
$u^3 - v^3 = q$ ("les deux nombres diffèrent du nombre donné.")
Donc

$$u^3 = \frac{q}{2} + \sqrt{\left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2} \qquad v^3 = -\frac{q}{2} + \sqrt{\left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2}$$

A l'aide de la formule de Tartaglia Cardan et son élève Ferrari font des progrès remarquables: résolution des différents cas cubiques, et même de l'équation du $4^{\text{ème}}$ degré (Ferrari, 1540 – voir § 4). Mais Cardan remarque très vite que le $2^{\text{ème}}$ cas $x^3 = px + q$ peu conduire à prendre la racine carrée d'un nombre négatif. Cardan pose la question à Tartaglia, qui lui répond de manière très désagréable:

« ... je vous réponds que vous n'avez pas maîtrisé la vraie manière de résoudre les problèmes de ce type; en fait je dirais que vos méthodes sont totalement fausses. »

En 1540 Cardan abandonne son poste à la Fondation Piatti pour permettre à Ferrari de prendre sa place. Pendant quelques années il se dédie au jeu (en particulier les échecs). En 1543 Cardan et Ferrari voyagent à Bologne, et découvrent les carnets de Scipione del Ferro. Cardan décide alors de publier la formule dans son *Ars magna* (1545), en citant les contributions de del Ferro et Tartaglia.

Tartaglia est furieux et insulte violemment Cardan, qui est maintenant reconnu comme le plus grand mathématicien de son temps. Ferrari répond à ces attaques en défiant Tartaglia. Celui-ci veut débattre avec Cardan, plus connu que son élève; il accepte finalement en 1548 un débat public avec Ferrari. Le débat a lieu dans une église à Milan, devant une grande foule comprenant les personnalités locales, y compris le gouverneur de Milan. A la fin du premier jour il est clair que Ferrari

maîtrise le sujet mieux que Tartaglia. Celui-ci quitte Milan à la nuit tombée et rentre à Venise, laissant la victoire à son rival.

Après la publication de son Ars magna Cardan va surtout exercer la médecine, obtenant là aussi une très grande célébrité – il est appelé par exemple en Écosse au chevet de l'archevêque de St-Andrews, avec succès. La fin de sa vie est triste: son fils aîné, coupable d'avoir empoisonné sa femme, est torturé et exécuté; son plus jeune fils, joueur et voleur, est banni; lui-même est emprisonné quelques mois par l'Inquisition.

La formule de Cardan et ses difficultés :

Pour l'équation écrite sous forme "moderne" $x^3 + px + q = 0$, la solution donnée par del Ferro-Tartaglia-Cardan est:

$$x = \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2}}$$

Cette formule pose cependant un certain nombres de problèmes:

a) Pour l'équation $x^3 + 16 = 12x$, la formule donne $x = \sqrt[3]{-8} + \sqrt[3]{-8} = -4$. Mais comment trouver la racine positive $x = 2$?

b) L'équation $x^3 + x = 2$ a une solution évidente $x = 1$. La formule donne:

$$x = \sqrt[3]{1 + \sqrt{\frac{28}{27}}} + \sqrt[3]{1 - \sqrt{\frac{28}{27}}}$$

qui, étant l'unique racine réelle de l'équation, est nécessairement égal à 1 – bien que ça ne saute pas aux yeux...

c) $x^3 = 15x + 4$. C'est le cas dit *irréductible* où la quantité $\left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2$ est négative. La formule donne $x = \sqrt[3]{2 + \sqrt{-121}} + \sqrt[3]{2 - \sqrt{-121}}$, alors que 4 est solution. Dans l'Ars magna Cardan traite un problème similaire avec des nombres imaginaires, mais il ne comprend pas réellement son calcul dont il dit qu'il est « aussi subtil qu'inutile ».

4. L'équation du 4ème degré et les débuts des nombres complexes

Lodovico Ferrari (1522–1565) arrive comme serviteur à l'âge de 14 ans chez Cardan. Celui-ci s'aperçoit vite des dons intellectuels du garçon et fait son éducation mathématique. Généreusement il laisse son poste d'enseignant à la fondation Piatti de Milan; Ferrari gagne facilement le concours et est nommé professeur en 1640, à 18 ans. C'est l'année où il résoud l'équation du 4ème degré $x^4 = ax^2 + bx + c$: il l'écrit sous la forme:

$$(x^2 + z)^2 = (a + 2z)x^2 + bx + (c + z^2)$$

et il choisit z de façon que le second membre soit de la forme $(\alpha x+\beta)^2$, c'est-à-dire que le discriminant $\Delta = b^2-4(a+2z)(c+z^2)$ soit nul. Cela donne une équation de degré 3 en z, que l'on résoud par la méthode de Cardan. α et β sont alors déterminés en fonction de z et de a,b,c, et l'équation devient

$$(x^2+\alpha x+\beta+z)(x^2-\alpha x-\beta+z)=0$$

qui se réduit à deux équations du second degré.

Ce résultat remarquable ne semble pas avoir impressioné Cardan. Il n'y consacre que quelques pages de l'*Ars Magna* qui traite en détail tous les cas possibles de l'équation du $3^{\text{ème}}$ degré. Dans la préface, Cardan explique qu'il est naturel de considérer les puissances 1,2 et 3, qui correspondent à une droite, une surface et un corps solide, mais qu'il ne serait « pas sage de dépasser ce point. La nature ne le permet pas ».

Rafaello Bombelli (1526-1572) est ingénieur hydraulique; une grande partie de sa carrière est consacrée à l'assèchement des marais dans le Val di Chiana, une région au Sud de la Toscane. Ces travaux subissent des interruptions fréquentes qui laissent à Bombelli le temps d'écrire son livre d'*Algèbre*, publié en 1572. Il utilise systématiquement les nombres négatifs, dont il énonce explicitement les règles de calcul. Il est le premier à raisonner avec des nombres complexes: il discute l'équation $x^3=15x+4$, le "cas irréductible". La formule de Cardan donne

$$x=\sqrt[3]{2+\sqrt{-121}}+\sqrt[3]{2-\sqrt{-121}}\ ,$$

alors que 4 est clairement une racine. Bombelli essaie de trouver la racine cubique de $2+\sqrt{-121}$ sous la forme $p+\sqrt{-q^2}$. En langage moderne, il s'agit de résoudre $(p+qi)^3=2+11i$. Il remarque que si l'on a trouvé une solution $p+qi$, on aura $(p-qi)^3=2-11i$; donc $2p=(p+qi)+(p-qi)$ sera solution de l'équation. Pour obtenir 4 il pose donc $p=2$ et cherche q tel que $(2+qi)^3=2+11i$, c'est-à-dire en développant:

$$8-6q^2=2\quad,\quad 12q-q^3=11\ .$$

La première équation donne $q=\pm 1$, mais seul $q=1$ satisfait aussi la deuxième. Donc une racine cubique de $2+11i$ est $2+i$, ce qui explique la formule de Cardan dans ce cas.

Bombelli indique les règles de calcul sur les nombres complexes; il introduit 4 notations de base, $piu=+1$, $meno=-1$, $piu\ di\ meno=i$, $meno\ di\ meno=-i$, et donne les règles de multiplication:
"Più via più di meno, fa più di meno .... Meno di meno via meno di meno, fa meno".

CHAPITRE III

Consolidation: 1570–1770

5. Les progrès de la notation algébrique

Bombelli est l'un des premiers à utiliser une notation algébrique, quoique plutôt incommode: $\sqrt[3]{2+11i}$ est écrit R.c.⌞ 2 p. di m. 11⌟, pour "racine cubique de [$2 + i \times 11$]".

L'invention de la notation algébrique moderne est souvent attribuée à François Viète (1540-1603). Viète était un mathématicien amateur; il a fait une carrière de conseiller politique d'abord à Rennes, puis à Paris, interrompue pendant 5 ans par les tensions dûes aux guerres de religion (Viète était protestant). C'est pendant cette période qu'il écrit son livre d'algèbre *In artem analyticam isagoge* ("Introduction à l'art analytique", 1591).

Ses notations sont encore assez loin des nôtres. Il est le premier à désigner les quantités par des lettres (voyelles pour les inconnues, consonnes pour les quantités connues). Mais il insiste bizarrement sur l'homogénéité des formules: la « première et perpétuelle loi des équations » est que « des termes homogènes doivent être comparés à des termes homogènes ». Chaque lettre reçoit donc une dimension, de façon que l'ensemble soit homogène. Ainsi l'équation $\mathrm{A}^3 + 3\mathrm{BA} = 2\mathrm{Z}$ (inconnue A, coefficients B et Z) est écrite:

Proponatur A cubus + B plano 3 in A aequari Z solido 2

pour marquer que B est une aire ("plano") et Z un volume ("solido").

C'est avec René Descartes (1596-1650) qu'apparaît une notation très proche de la notation actuelle: $a, b, c \ldots$ désignent les quantités connues, $x, y, z \ldots$ inconnues; les puissances sont notées comme maintenant. Deux exceptions: il utilise xx plutôt que x^2, et le signe ∞ pour l'égalité, bien que le symbole = ait été introduit en 1557 par Recorde.

Descartes est un homme universel: philosophie, physique (optique en particulier), cosmologie, mécanique... et mathématiques. Son travail en algèbre est essentiellement contenu dans le livre III de *la Géométrie* (1637), qui est elle-même l'un des 3 appendices du célèbre Discours de la Méthode.

6. Le nombre de racines d'une équation

L'idée qu'une équation du $3^{\text{ème}}$ degré peut avoir 3 solutions n'apparaît pas chez les italiens, tout simplement parce qu'ils ne considèrent que des équations qui ont au plus 2 racines positives (voir § 3). Le premier à énoncer qu'une équation de degré n a n racines est Albert Girard (1595–1632), un mathématicien né en France mais émigré en Hollande, dans *L'invention en algèbre* (1629). Mais il lui faut bien

sûr admettre des racines "impossibles", et ce qu'il entend par là n'est pas clair. Néanmoins il énonce les relations entre racines et coefficients (voir § 7).

Descartes donne un énoncé du même type:

« Au reste tant les vraies racines (= positives) que les fausses (= négatives) ne sont pas toujours réelles, mais quelquefois seulement imaginaires, c'est-à-dire qu'on peut bien toujours en imaginer autant que j'ai dit en chaque équation, mais qu'il n'y a quelquefois aucune quantité qui corresponde à celle qu'on imagine ».

Descartes compte aussi les racines *positives* ("vraies") d'une équation:

Règle des signes de Descartes .– *Soit* p *le nombre de racines* >0 *de l'équation* $f(x)=a_0x^n+\ldots+a_n=0$ *, et soit* c *le nombre de changement de signes dans la suite* $(a_0,\ldots,a_n)$ *(on n'écrit pas les* a_i *égaux à zéro). Alors* $p\leq c$ *, et* $p\equiv c$ (mod. 2).

Exemple : si $q<0$, l'équation $x^3+px+q=0$ a exactement une solution >0 (pourquoi?).

Descartes n'indique pas de démonstration; en voici une. On démontre d'abord la congruence $p\equiv c$ (mod. 2). En remplaçant f par $-f$ on ne change ni les racines, ni c ; on peut donc supposer $a_0>0$. Après le k-ième changement de signe, le signe du coefficient est $(-1)^k$; on en déduit que le signe de $a_n=f(0)$ est $(-1)^c$. Si $f(0)>0$, comme $f(x)\to+\infty$ quand $x\to+\infty$, la courbe $y=f(x)$ traverse un nombre pair de fois l'axe des x sur $[0,+\infty[$ (il faut affiner un peu l'argument si f a des racines multiples). De même si $f(0)<0$ le nombre p de racines positives est impair. Cela démontre que p et c ont la même paritéé.

On démontre alors l'inégalité $p\leq c$ par récurrence sur le degré n de f . Le cas $n=1$ est facile. Soient p' , c' les nombres de racines positives et de changement de signes pour la dérivée f' de f . La suite des coefficients de f' est $(na_0,\ldots,a_{n-1})$; on a donc $c'=c$ ou $c-1$. D'autre part entre deux racines de f f' a au moins une racine (théorème de Rolle), donc $p'\geq p-1$, soit

$$p\leq p'+1\leq c'+1\leq c+1$$

(la deuxième inégalité vient de l'hypothèse de récurrence). Mais comme p et c ont la même parité, on en déduit $p\leq c$. ∎

7. Relations entre les racines et les coefficients

Après 1650 l'idée qu'une équation de degré n a n racines "imaginaires" (comptées avec multiplicité) est largement admise, même si la définition d'"imaginaire" reste très imprécise. On peut considérer que l'énoncé moderne correspondant est le suivant:

Théorème de décomposition .– *Étant donné un corps* K *et un polynôme* P(X) *dans* K[X] *, il existe un corps* L *contenant* K *et des éléments* $\alpha_1,\ldots,\alpha_n$ *de* L *tels*

que

$$\mathrm{P}(\mathrm{X}) = (\mathrm{X} - \alpha_1) \dots (\mathrm{X} - \alpha_n) \ .$$

Démonstration : Il suffit de trouver *une* racine, disons α, de P dans un corps K_1 contenant K : en effet, $\mathrm{P}(\mathrm{X})$ est alors divisible par $(\mathrm{X} - \alpha)$ (Descartes), donc s'écrit $(\mathrm{X} - \alpha)\mathrm{P}_1(\mathrm{X})$ avec $\mathrm{P}_1 \in \mathrm{K}_1[\mathrm{X}]$. On trouve alors un corps K_2 contenant K_1 dans lequel P_1 a une racine; comme le degré descend d'un à chaque fois, en n étapes on arrive à la situation cherchée.

Pour construire K_1, on peut supposer que P est irréductible, c'est-à-dire ne se décompose pas en produit de polynômes (sinon on applique ce qui suit à un facteur irréductible de P). On construit K_1 en "adjoignant" à K un élément α qui satisfait $\mathrm{P}(\alpha) = 0$, de même qu'on construit $\mathbb{C}$ en adjoignant à $\mathbb{R}$ un élément i qui satisfait $i^2 + 1 = 0$. De manière précise, on prend pour L l'anneau des polynômes modulo P, qui se définit de la même manière que celui des entiers modulo p : on part de l'anneau $\mathrm{K}[\mathrm{X}]$, et on identifie deux polynômes qui diffèrent par un multiple de P. Il est donc formé des polynômes $a_0 + a_1 x + \ldots + a_{n-1}x^{n-1}$ avec l'addition habituelle; le produit de deux tels polynômes A et B est le reste de la division de AB par P. Si $\mathrm{A} \neq 0$, le théorème de Bezout affirme qu'il existe $\mathrm{B}, \mathrm{C} \in \mathrm{K}[\mathrm{X}]$ tels que $\mathrm{AB} + \mathrm{CP} = 1$, autrement dit $\mathrm{AB} \equiv 1 \pmod{\mathrm{P}}$. Cela prouve que l'anneau L est un corps. Il contient K, identifié à l'ensemble des polynômes constants. Enfin dans L l'élément x vérifie $\mathrm{P}(x) = 0$, donc est une racine de P. ∎

Remarques.– 1) On prendra garde de distinguer ce résultat du *théorème fondamental de l'algèbre* (voir § 9), qui affirme que si $\mathrm{K} = \mathbb{C}$ le résultat ci-dessus est vérifié en prenant $\mathrm{L} = \mathbb{C}$. Le théorème de décomposition est beaucoup plus faible puisqu'il nécessite d'agrandir le corps de base d'une manière qui dépend étroitement du polynôme considéré.

2) Écrivons $\mathrm{P}(\mathrm{X}) = \mathrm{X}^n + a_1\mathrm{X}^{n-1} + \ldots + a_n$. En développant l'égalité du théorème on obtient $a_p = (-1)^p \, \mathrm{S}_p(\alpha_1, \ldots, \alpha_n)$, où $\mathrm{S}_1, \ldots \mathrm{S}_n$ sont les *fonctions symétriques élémentaires* :

$$\mathrm{S}_p(\mathrm{X}_1, \ldots \mathrm{X}_n) = \sum_{i_1 < \ldots < i_p} \mathrm{X}_{i_1} \ldots \mathrm{X}_{i_p} \ .$$

Cette égalité, déjà connue de Girard, va jouer un rôle important dans la suite.

Vers 1666 Newton[3] exprime d'autres fonctions symétriques des racines, les *sommes de Newton* $\sigma_k = \alpha_1^k + \ldots + \alpha_n^k$ en fonction des a_i :

$$\sigma_1 = -a_1 \quad , \quad \sigma_2 = a_1^2 - 2a_2 \quad , \quad \sigma_3 = -a_1^3 + 3a_1a_2 - 3a_3 \quad , \text{etc.}$$

[3] Isaac Newton (1643–1727) est un des grands savants de son temps: physicien (gravitation, optique) et mathématicien (découverte du calcul infinitésimal, en concurrence avec Leibnitz).

En fait Newton donne une formule de récurrence pour calculer σ_k :

$$0 = \begin{cases} \sigma_k + a_1\sigma_{k-1} + \ldots + a_{k-1}\sigma_1 + ka_k & \text{si} \quad k \leq n \ ; \\ \\ \sigma_k + a_1\sigma_{k-1} + \ldots + a_n\sigma_{k-n} & \text{si} \quad k > n \ . \end{cases}$$

Il ne donne pas de démonstration; elle peut s'obtenir par exemple en développant en série l'égalité $\mathrm{P}'(x) = \mathrm{P}(x) \sum \dfrac{1}{x - \alpha_i}$.

Le fait que tout polynôme symétrique est un polynôme en les S_p semble avoir été énoncé pour la première fois par Waring[4] en 1770, bien qu'il ait été certainement connu bien avant. Voici la démonstration de Waring, et d'abord l'énoncé:

Théorème .– *Tout polynôme* $\mathrm{P} \in k[\mathrm{X}_1, \ldots \mathrm{X}_n]$ *symétrique est égal à un polynôme en* $\mathrm{S}_1, \ldots, \mathrm{S}_n$.

(Un polynôme $\mathrm{P} \in k[\mathrm{X}_1, \ldots \mathrm{X}_n]$ est *symétrique* s'il est invariant lorsqu'on fait une permutation quelconque des variables.)

Démonstration : on munit $\mathbb{N}^n$ de l'ordre lexicographique: $(p_1, \ldots, p_n) \geq (q_1, \ldots, q_n)$ si $p_1 > q_1$, ou $p_1 = q_1$ et $p_2 > q_2$, etc. On définit le degré $\deg(\mathrm{P})$ d'un polynôme P comme le plus grand n-uple $(p_1, \ldots, p_n)$ tel que le monôme $\mathrm{X}_1^{p_1} \ldots \mathrm{X}_n^{p_n}$ apparait dans P . On a

$$\deg(\mathrm{S}_1) = (1, 0, \ldots, 0) \quad \deg(\mathrm{S}_2) = (1, 1, 0, \ldots, 0) \quad \deg(\mathrm{S}_n) = (1, 1, \ldots, 1)$$
$$\deg(\mathrm{PQ}) = \deg(\mathrm{P}) + \deg(\mathrm{Q}) \quad , \quad \deg(\mathrm{P} + \mathrm{Q}) \leq \max\left(\deg(\mathrm{P}), \deg(\mathrm{Q})\right) \ .$$

On fait alors la démonstration par récurrence sur $\deg(\mathrm{P})$. Soit P un polynôme symétrique, de degré $(p_1, \ldots, p_n)$. Alors $p_1 \geq p_2 \geq \ldots \geq p_n$: en effet le monôme $\mathrm{X}_1^{p_1} \ldots \mathrm{X}_n^{p_n}$ apparaît dans P , donc aussi le monôme obtenu en permutant X_1 et X_2 ; le degré $(p_2, p_1, \ldots, p_n)$ de celui-ci doit être $\leq (p_1, \ldots, p_n)$, d'où $p_1 \geq p_2$. En permutant de même X_i et X_{i+1} , on obtient $p_i \geq p_{i+1}$.

On considère alors le polynôme symétrique $\mathrm{S} = \mathrm{S}_1^{p_1 - p_2} \mathrm{S}_2^{p_2 - p_3} \ldots \mathrm{S}_n^{p_n}$. Le monôme de plus haut degré de S est $\mathrm{X}_1^{p_1} \ldots \mathrm{X}_n^{p_n}$, qui apparaît avec coefficient 1. Donc si $\mathrm{P} = a\mathrm{X}_1^{p_1} \ldots \mathrm{X}_n^{p_n} +$ termes de degré plus bas, le polynôme $\mathrm{P} - a\mathrm{S}$ est de degré $< \deg(\mathrm{P})$ et symétrique, donc un polynôme en les S_p par l'hypothèse de récurrence. ∎

On en déduit facilement le même résultat pour les *fractions rationnelles*, c'est-à-dire les fractions $\frac{\mathrm{P}}{\mathrm{Q}}$ où $\mathrm{P}, \mathrm{Q} \in \mathrm{K}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$: *toute fraction rationnelle* symétrique *est égale à une fraction rationnelle en* $\mathrm{S}_1, \ldots, \mathrm{S}_n$.

[4] Edward Waring (1736-1798), Professeur de Mathématiques à Cambridge, est un personnage assez curieux. Il a obtenu, ou au moins énoncé, beaucoup de résultats nouveaux mais il écrivait de manière si lourde et obscure que ses travaux n'ont guère été reconnus.

8. Autres méthodes pour les équations de degré 3 et 4

Dans la période un certain nombre d'approches alternatives sont trouvées pour résoudre les équations du $3^{\text{ème}}$ et $4^{\text{ème}}$ degré, le plus souvent avec l'espoir qu'elles se généraliseront en degré plus grand. Je discute ci-dessous celles de Descartes et Tschirnhaus; Euler et Bezout en ont également proposées.

Descartes

Descartes utilise systématiquement la décomposition des polynômes en facteurs. Il est le premier à écrire explicitement qu'un polynôme P est divisible par $\mathrm{X}-a$ si et seulement si $\mathrm{P}(a)=0$. Plus généralement, il développe l'idée de réduire la complexité d'une équation $\mathrm{P}=0$ en décomposant P comme produit de polynômes. Il obtient ainsi entre autres une nouvelle méthode pour l'équation du $4^{\text{ème}}$ degré. Il explique d'abord en détail qu'une translation sur x permet de réduire l'étude d'une équation de degré n au cas où le coefficient de x^{n-1} est nul. Il considère alors le polynôme $\mathrm{P}(x)=x^4+px^2+qx+r$, qu'il propose de factoriser en produit de polynômes du second degré:

$$x^4+px^2+qx+r=(x^2+ax+b)(x^2-ax+c)$$

Cela impose:

$$b+c-a^2=p \quad , \quad a(c-b)=q \quad , \quad bc=r \ ,$$
$$\text{d'où} \quad b=\frac{1}{2}(a^2+p-\frac{q}{a}) \quad , \quad c=\frac{1}{2}(a^2+p+\frac{q}{a}) \ ,$$
$$\text{et en reportant dans } \ bc=r: \quad a^6+2pa^4+(p^2-4r)a^2-q^2=0$$

qui est une équation du $3^{\text{ème}}$ degré en a^2.

Noter que les mathématiciens de l'époque sont loin de maîtriser ce type de calculs: une erreur fameuse de Leibnitz[5] (1702) est d'affirmer que le polynôme x^4+1 est irréductible sur $\mathbb{R}$, alors que

$$x^4+1=(x^2+1)^2-2x^2=(x^2+\sqrt{2}x+1)(x^2-\sqrt{2}x+1) \ .$$

Tschirnhaus

Étant donné une équation $x^n+a_1x^{n-1}+\ldots+a_n=0$, le changement de variable $y=x+\frac{a_1}{n}$ permet de se ramener au cas $a_1=0$ – ce point est expliqué en détail dans la *Géométrie* de Descartes. En 1683, le mathématicien allemand Tschirnhaus [6]

[5] Gottfried von Leibnitz (1646-1716) est, comme Descartes, philosophe, mathématicien, physicien, ... Sa grande œuvre mathématique est l'invention du calcul infinitésimal, en concurrence avec Newton.

propose de pousser cette méthode plus loin. Expliquons son idée en termes modernes, en considérant le changement de variable $y = u_0 + u_1 x + u_2 x^2$. Alors y vérifie une équation $y^n + b_1 y^{n-1} + \ldots + b_n = 0$, dont les coefficients b_i sont des polynômes en $a_1, \ldots, a_n$: en effet toute fonction symétrique élémentaire de $y_i = u_0 + u_1 x_i + u_2 x_i^2$ est une fonction symétrique des x_i . Par exemple:

$$b_1 = -\sum_i (u_0 + u_1 x_i + u_2 x_i^2) = -n u_0 + a_1 u_1 + (2a_2 - a_1^2) u_2 \ , \text{ etc.}$$

$a_1, \ldots, a_n$ étant fixés, on peut déterminer u_0, u_1, u_2 non tous nuls de façon que $b_1 = b_2 = 0$: la première condition donne u_0 comme fonction linéaire de u_1 et u_2 , en reportant dans la seconde on trouve une équation $a u_1^2 + b u_1 u_2 + c u_2^2 = 0$, où a, b, c sont des polynômes en $a_1, \ldots, a_n$. En extrayant une racine carrée on trouve une solution non nulle pour (u_1, u_2) , d'où on déduit u_1 . Si maintenant on connaît une racine, disons y_1 , de l'équation $y^n + b_1 y^{n-1} + \ldots + b_n = 0$, la racine x_1 correspondante est solution de $u_2 x_1^2 + u_1 x_1 + u_0 = y_1$.

Exemples .– 1) Moyennant une extraction de racine carrée on réduit l'équation du $3^{\text{ème}}$ degré à $y^3 = b$, que l'on résoud moyennant l'extraction d'une racine cubique. On peut vérifier que cette procédure redonne la formule de Cardan.

2) L'équation du $4^{\text{ème}}$ degré se ramène à la forme $x^4 + px + q = 0$, ce qui malheureusement ne suffit pas à la résoudre...

Tschirnhaus semble avoir cru que la même méthode, avec un polynôme $u_0 + u_1 x + \ldots + u_m x^m$ de degré > 2 , permettrait de résoudre des équations de degré plus grand et notamment celle du $5^{\text{ème}}$ degré. Leibniz lui fait alors remarquer que les équations auxiliaires en les u_i vont être de degré > 5 , de sorte que la méthode ne peut réussir (échange de lettres vers 1680). Notons cependant qu'elle permet de réduire l'équation du $5^{\text{ème}}$ degré à la forme $x^5 + px + q = 0$ (la preuve demande un peu de géométrie algébrique); ce résultat a été utilisé au $19^{\text{ème}}$ siècle pour résoudre l'équation de degré 5 en se permettant d'utiliser certaines fonctions (relativement) simples, appelées *fonctions elliptiques* (Kronecker, Hermite).

CHAPITRE IV

L'âge d'or: 1770–1830

[6] Ehrenfried Tschirnhaus (1651–1708) a fait ses études supérieures à Leiden. Il est surtout connu pour la méthode indiquée ici; il est aussi l'auteur d'un nouveau procédé de fabrication de la porcelaine.

9. Le théorème fondamental de l'algèbre

L'"âge d'or" évoqué dans le titre de ce chapitre commence en 1770 avec le mémoire de Lagrange, puis les travaux de Ruffini, Abel et enfin Galois qui mènent à une compréhension complète du sujet.

Je vais commencer par un résultat important démontré au début de cette période; il est de nature un peu différente dans la mesure où il fait appel à la structure particulière de $\mathbb{R}$, donc à l'analyse. Il s'agit du théorème suivant:

Théorème fondamental de l'algèbre .– *Tout polynôme* $\mathrm{P} \in \mathbb{C}[\mathrm{X}]$ *se décompose en produit de facteurs du premier degré.*

La première tentative de démonstration est dûe à d'Alembert[7] en 1746; basée sur l'analyse, elle comporte de grosses lacunes. Euler[8] propose en 1749 une démonstration algébrique, dans l'esprit de la résolution par Descartes de l'équation du $4^{\text{ème}}$ degré, mais ce n'est qu'une esquisse très insuffisante. Lagrange (voir § 10) donne une preuve complète en 1772, mais en admettant, comme il était d'usage (voir § 7), l'existence de n racines "imaginaires". Dans sa thèse (1799), Gauss[9] critique les démonstrations de ses prédécesseurs, puis donne lui-même une démonstration géométrique assez obscure et d'une rigueur laissant à désirer. Il y revient en 1816 avec deux démonstrations tout-à-fait inattaquables. Voici l'une d'elles, qui reprend l'idée d'Euler:

Démonstration : D'abord deux réductions. Comme pour la démonstration du théorème de décomposition, il suffit de prouver que P admet *un* zéro complexe. Écrivons $\mathrm{P}(\mathrm{X}) = \mathrm{X}^n + a_1\mathrm{X}^{n-1} + \ldots + a_n$, avec $a_1, \ldots, a_n \in \mathbb{C}$. Notons $\bar{\mathrm{P}}$ le polynôme $\mathrm{X}^n + \bar{a}_1\mathrm{X}^{n-1} + \ldots + \bar{a}_n$. Le polynôme $\mathrm{P}\bar{\mathrm{P}}$ est à coefficients réels. S'il admet un zéro $\alpha \in \mathbb{C}$, on a ou bien $\mathrm{P}(\alpha) = 0$, ou bien $\bar{\mathrm{P}}(\alpha) = 0$, ce qui est équivalent par conjugaison complexe à $\mathrm{P}(\bar{\alpha}) = 0$. Ainsi, *il suffit de prouver que tout polynôme* $\mathrm{P} \in \mathbb{R}[\mathrm{X}]$ *admet un zéro dans* $\mathbb{C}$.

Écrivons $n = 2^e m$, où m est impair. La démonstration se fait par récurrence sur e. Si $e = 0$, quand x varie de $-\infty$ à $+\infty$ $\mathrm{P}(x)$ fait de même, et donc s'annule au moins une fois.

---

[7] Jean D'ALEMBERT (1717–1783) est surtout connu des mathématiciens pour ses travaux en mécanique, et du reste du monde pour l'énorme travail que représente l'*Encyclopédie*, dont il a été avec Diderot l'un des principaux contributeurs.

[8] Leonhard EULER (1707–1783) est probablement le plus grand mathématicien du $18^{\text{ème}}$ siècle. Après des études à Bâle, il a fait toute sa carrière à l'Académie des Sciences de Saint-Petersbourg, avec un intermède de 15 ans à celle de Berlin. Ses contributions essentielles sont en analyse, en géométrie, en théorie des nombres, en mécanique.

[9] Carl Friedrich GAUSS (1777–1855) est un physicien et astronome au moins autant que mathématicien – il a fait toute sa carrière à Göttingen comme directeur de l'Observatoire. Il a néanmoins obtenu des résultats de premier ordre en théorie des nombres, géométrie différentielle, équations différentielles, ...

Supposons $e \geq 1$. Choisissons un corps $\mathrm{L} \supset \mathbb{C}$ dans lequel $\mathrm{P(X)} = (\mathrm{X} - x_1) \dots (\mathrm{X} - x_n)$ (théorème de décomposition). Soit $t \in \mathbb{R}$; posons $y_{ij} = x_i + x_j + t x_i x_j$ pour $1 \leq i < j \leq n$, et $\mathrm{Q(Y)} = \prod_{i<j} (\mathrm{Y} - y_{ij})$. Toute permutation des x_i se traduit par une permutation des y_{ij}, donc les polynômes symétriques en les y_{ij} sont aussi des polynômes symétriques en les x_i. Par conséquent les coefficients de Q sont des polynômes en les coefficients de P, donc des nombres réels. On a

$$\deg(\mathrm{Q}) = \frac{1}{2} n(n-1) = 2^{e-1}(2^e m - 1) \ .$$

Par l'hypothèse de récurrence Q a au moins une racine dans $\mathbb{C}$: il existe i, j (dépendant de t) tels que $x_i + x_j + t x_i x_j \in \mathbb{C}$.

Faisons varier t dans $\mathbb{R}$: comme il n'y a qu'un nombre fini de couples (i, j) on peut trouver deux valeurs distinctes t et t' correspondant au même couple (i, j). On a donc

$$x_i + x_j + t x_i x_j \in \mathbb{C} \quad , \quad x_i + x_j + t' x_i x_j \in \mathbb{C} \ ,$$

d'où l'on déduit $x_i + x_j = p \in \mathbb{C}$ et $x_i x_j = q \in \mathbb{C}$. Ainsi x_i et x_j sont les racines de l'équation $x^2 - px + q = 0$, et donc appartiennent à $\mathbb{C}$. ∎

10. Lagrange

Joseph-Louis Lagrange (= Giuseppe Lodovico Lagrangia, 1736–1813) est considéré en France comme un mathématicien français, en Italie comme un mathématicien italien. Il est né à Turin et y a fait ses études, d'ailleurs peu avancées – il est assez largement autodidacte. Il commence une correspondance avec Euler qui est impressionné par ce jeune garçon; à 20 ans il est élu membre de l'Académie des Sciences de Berlin, et il en devient directeur pour les Mathématiques à 30 ans. Il y reste 20 ans, puis accepte un poste prestigieux à l'Académie des Sciences de Paris. Dans les années 1795 il enseigne à l'École Polytechnique et à l'École Normale Supérieure, nouvellement créées; il n'est apparemment pas très apprécié, il a une voix faible et un fort accent italien. Il termine sa vie dans les honneurs: comte d'Empire, légion d'honneur...

En 1770 Lagrange publie ses *Réflexions sur la résolution algébrique des équations*. Il décrit son objet comme suit:

« Je me propose dans ce Mémoire d'examiner les différentes méthodes que l'on a trouvées jusqu'à présent pour la résolution algébrique des équations, de les réduire à des principes généraux, et de faire voir *à priori* pourquoi ces méthodes réussissent pour le troisième et le quatrième degré, et sont en défaut pour les degrés ultérieurs ».

Voici par exemple comment Lagrange analyse la formule de Cardan. Rappelons que pour résoudre l'équation $x^3 + px + q = 0$ on pose $x = u + v$ avec $3uv + p = 0$,

de sorte que l'équation devient $u^3 + v^3 + q = 0$. Autrement dit, la variable auxiliaire u vérifie l'équation

$$u^3 - \big(\frac{p}{3u}\big)^3 + q = 0 \quad , \quad \text{soit} \quad u^6 + qu^3 - \big(\frac{p}{3}\big)^3 = 0 \ ,$$

qui est quadratique en u^3 , donc que l'on sait résoudre. Cette équation, que Lagrange appelle l'équation *réduite*, admet 6 solutions, que l'on peut écrire

$$u_0 \ , \ \rho u_0 \ , \ \rho^2 u_0 \ ; \ u_1 \ , \ \rho u_1 \ , \ \rho^2 u_1 \ .$$

Les racines de l'équation originale sont alors:

$$x_1 = u_0 + u_1 \quad , \quad x_2 = \rho u_0 + \rho^2 u_1 \quad , \quad x_3 = \rho^2 u_0 + \rho u_1 \ .$$

Maintenant Lagrange détermine les u_i en fonction des x_i . Comme $1 + \rho + \rho^2 = 0$, on trouve:

$$u_0 = \frac{1}{3}(x_1 + \rho x_2 + \rho^2 x_3) \quad , \quad u_1 = \frac{1}{3}(x_1 + \rho^2 x_2 + \rho x_3) \ ;$$

ainsi les 6 racines de l'équation réduite sont obtenues à partir de l'expression $\frac{1}{3}(x_1 + \rho x_2 + \rho^2 x_3)$ en effectuant les 6 permutations de $\{x_1, x_2, x_3\}$.

La remarque clé de Lagrange est la suivante:

Proposition .– *Supposons que le polynôme* $\mathrm{P} \in k[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ *prenne* m *valeurs différentes* $\mathrm{P}_1, \ldots, \mathrm{P}_m$ *quand on permute les variables. Alors* P *vérifie une équation* $\mathrm{Y}^m + b_1 \mathrm{Y}^{m-1} + \ldots + b_0 = 0$ *, où* $b_1, \ldots, b_m$ *sont des polynômes symétriques en les* X_i .

Démonstration : Considérons le polynôme $(\mathrm{Y} - \mathrm{P}_1) \ldots (\mathrm{Y} - \mathrm{P}_m)$ en une indéterminée Y , à coefficients dans $k[\mathrm{X}_1, \ldots, \mathrm{X}_n]$. Il annule P (qui est égal à l'un des P_i), et ses coefficients sont des polynômes symétriques. ∎

Revenant à l'équation du 3ème degré, on obtient *a priori* que

- $u_0 = \frac{1}{3}(x_1 + \rho x_2 + \rho^2 x_3)$ satisfait une équation de degré 6;
- $u_0^3 = \frac{1}{3}(x_1 + \rho x_2 + \rho^2 x_3)^3$ satisfait une équation de degré 2.

Étudiant ensuite la méthode de Ferrari pour l'équation du 4ème degré, Lagrange trouve qu'elle fait intervenir le polynôme $x_1 x_2 + x_3 x_4$ en les 4 racines; celui-ci ne prend que 3 valeurs par permutations, ce qui explique pourquoi la méthode marche. Noter que celle-ci donne un moyen explicite (un peu lourd, certes) d'écrire l'équation réduite, donc de résoudre l'équation originale.

Dans la situation de la proposition, Lagrange montre que le nombre m est égal à $n!/\mathrm{I(P)}$, où $\mathrm{I(P)}$ est le nombre des permutations qui laisse P invariant. Interprété en langage moderne, c'est le "théorème de Lagrange": l'ordre d'un sous-groupe divise l'ordre du groupe. On peut déduire facilement du travail de Lagrange

que les méthodes de Cardan, Ferrari, Descartes... ne peuvent se généraliser en degré plus grand. Cela ne prouve pas bien sûr qu'il n'existe pas d'autres, et l'opinion de Lagrange à ce sujet n'est pas claire:

"Il serait à propos d'en faire l'application aux équations du cinquième degré et des degrés supérieurs, dont la résolution est jusqu'à présent inconnue; mais cette application demande un trop grand nombre de recherches et de combinaisons, dont le succès est d'ailleurs fort douteux, pour que nous puissions quant à présent nous livrer à ce travail."

11. Ruffini et Abel

Les méthodes de Lagrange sont poussées plus loin par Paolo Ruffini (1765–1822). Ruffini reçoit à l'Université de Modène une double formation en médecine et Mathématiques; il devient lui-même professeur à Modène en 1791. En 1799 il publie un gros traité de 516 pages: *Teoria generale delle equazioni, in cui si dimostra impossibile la soluzione algebraica delle equazioni generali di grado superiore al* 4^{o}.

Le moins qu'on puisse dire est que le travail de Ruffini n'a pas été reçu avec enthousiasme. Il était apparemment très difficile à lire. Ruffini a réécrit plusieurs fois sa démonstration, sans arriver à convaincre ses contemporains. De fait il semble qu'en dépit de nombreuses idées originales, ses différentes preuves aient achoppé sur une difficulté importante qu'on va expliquer ci-dessous.

En tout cas Ruffini a le mérite de lancer l'idée que l'équation générale du $5^{\text{ème}}$ degré n'est pas résoluble par radicaux. Une démonstration convaincante devait être obtenue en 1824 par Abel.

Niels Abel (1802–1829) vient d'une famille peu fortunée de Norvège – toute sa vie sera une lutte contre la pauvreté. Un jeune professeur de mathématiques de son lycée, Holmboe, découvre ses dons et convainc ses collègues de se cotiser pour lui payer l'Université. Le travail sur les équations de degré ≥ 5 est le premier "grand" résultat d'Abel; il le fait publier lui-même à ses frais, et du coup en réduit la taille au maximum: 6 pages!

Après ce coup d'éclat Abel obtient des résultats encore plus profonds, sur ce qu'on appelle maintenant les *intégrales abéliennes*. Ce travail, qu'il essaie de faire connaître en Allemagne et en France, obtient peu d'échos: Cauchy égare le manuscrit. De 1825 à 1827, Abel voyage entre la France et l'Allemagne en essayant de faire connaître ses travaux, sans guère de succès. Il y épuise sa santé et le peu d'argent qui lui reste. Il doit rentrer en Norvège, où il devient sérieusement malade (tuberculose). À Noël 1828, un voyage en traîneau à Froland, au sud de la Norvège, où travaille sa fiancée, aggrave son état; il meurt trois mois plus tard. Quelques jours après arrive une lettre de Berlin lui proposant un poste de Professeur à l'Université.

Voici une idée de la démonstration d'Abel. Il considère l'équation *générale* $x^n + a_1 x^{n-1} + \ldots + a_n = 0$; cela signifie que l'on voit $a_1, \ldots, a_n$ comme des indé-

terminées, ainsi que les racines $x_1, \ldots, x_n$ de l'équation. Ces deux n-uples d'indéterminées sont liées par la relation

$$x^n + a_1 x^{n-1} + \ldots + a_n = (\mathrm{X} - x_1) \ldots (\mathrm{X} - x_n)$$

ou, de manière équivalente, $(-1)^p a_p = \mathrm{S}_p(x_1, \ldots x_n)$ pour tout n. En particulier, d'après le théorème des fonctions symétriques, $\mathbb{C}(a_1, \ldots, a_n)$ est le sous-corps de $\mathbb{C}(x_1, \ldots, x_n)$ formé des fractions rationnelles symétriques.

Dire que l'équation est résoluble par radicaux, c'est dire que l'on peut trouver une suite de corps

$$\mathrm{K}_0 = \mathbb{C}(a_1, \ldots, a_n) \subset \mathrm{K}_1 \subset \ldots \subset \mathrm{K}_r$$

de façon qu'au moins une des racines, par exemple x_1, appartient à K_r, et que chaque corps K_{i+1} s'obtienne à partir de K_i en extrayant une racine. Par exemple K_1 est obtenu en adjoignant à $\mathrm{K}_0 = \mathbb{C}(a_1, \ldots, a_n)$ un élément u tel que $u^p = f(a_1, \ldots, a_n) \in \mathrm{K}_0$, pour un certain entier p; K_2 en adjoignant à K_1 un élément v tel que $v^q \in \mathrm{K}_1$, pour un certain entier q, etc.

Admettons alors un point délicat de la démonstration[10] : on peut prendre les K_i dans le corps $\mathbb{C}(x_1, \ldots, x_n)$. Autrement dit, on peut prendre pour $u, v, \ldots$ des fractions rationnelles en $x_1, \ldots, x_n$. Pour toute permutation σ de $[1, n]$, notons $\sigma(u)$ la fraction rationnelle $u(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$. Comme les éléments de K_0 sont symétriques, on a $\sigma(u^p) = u^p$ et par conséquent

$$\sigma(u) = \lambda(\sigma) u \ , \quad \text{avec} \ \ \lambda(\sigma)^p = 1 \ .$$

Si maintenant τ est une autre permutation, on trouve en appliquant τ à l'égalité précédente:

$$\tau(\sigma(u)) = \tau(\lambda(\sigma)u) = \lambda(\sigma)\tau(u) = \lambda(\sigma)\lambda(\tau)u \ , \quad \text{d'où} \ \ \lambda(\tau\sigma) = \lambda(\tau)\lambda(\sigma) \ .$$

Supposons alors $n \geq 5$, et prenons[11] $\sigma = (123)$ et $\tau = (345)$. On a $\sigma^3 = \tau^3 = \mathrm{Id}$, d'où $\lambda(\sigma)^3 = \lambda(\tau)^3 = 1$. Mais $\tau\sigma = (12453)$ est d'ordre 5, donc $\lambda(\tau\sigma)^5 = 1$. Cela n'est possible que si $\lambda(\sigma) \cdot \lambda(\tau) = 1$. Appliquant le même raisonnement en remplaçant σ par $\sigma^2 = (132)$, on trouve aussi $\lambda(\sigma)^2 \cdot \lambda(\tau) = 1$, d'où finalement $\lambda(\sigma) = \lambda(\tau) = 1$.

Ainsi u est invariant par les permutations σ et τ; il en résulte que tous les éléments de K_1 possèdent cette propriété d'invariance. De proche en proche le même

[10] C'est ce point qui ne semble pas être correctement traité par Ruffini.

[11] On note (123) la permutation qui envoie 1 sur 2, 2 sur 3, 3 sur 1, et qui laisse les autres entiers fixes.

argument montre que tous les éléments de K_2, puis K_3, ... , puis K_r sont invariants par σ et τ. Mais K_r contient x_1 qui n'est pas invariant par σ, d'où une contradiction. ∎

Ainsi l'équation générale de degré ≥ 5 n'est pas résoluble par radicaux; d'un autre côté, Gauss et Abel lui-même avaient donné d'importants exemples d'équations particulières qui le sont. Il devenait donc très naturel de chercher à caractériser les équations résolubles par radicaux. On sait qu'Abel y travaillait peu avant sa mort; mais c'est Galois qui devait résoudre définitivement le problème – et du même coup éclairer d'un jour nouveau la théorie des équations algébriques.

12. Galois

Évariste Galois (1811–1832) est né à Bourg-la-Reine dans une famille bourgeoise et républicaine (son père est élu maire de Bourg-la-Reine en 1815). Il entre à Louis-le-Grand, où il stupéfie son professeur de Mathématiques, Mr. Richard. Il publie ses premiers articles, dont un sur la théorie des équations qu'il envoie à l'Académie des Sciences; il sera perdu par Cauchy.

En 1829 les difficultés s'accumulent. Son père se suicide à la suite d'une cabale montrée contre lui par le curé de Bourg-la-Reine. Il est recalé au Concours d'entrée à Polytechnique (la légende veut qu'il ait jeté le chiffon à craie à la figure de l'examinateur). Il entre alors à l'École Normale, où il rédige son mémoire *Conditions pour qu'une équation soit résoluble par radicaux* afin de concourir au grand prix de mathématiques de l'Académie des Sciences. Fourier emporte le manuscrit chez lui et meurt peu après : le manuscrit est perdu, et le grand prix est décerné à Abel (mort l'année précédente) et à Jacobi.

Les normaliens, consignés dans leur école, ne peuvent participer aux journées révolutionnaires de 1830; mais Galois commence à développer une activité politique intense. Après avoir dénoncé dans la Gazette des écoles le directeur de l'École Normale et la médiocrité de l'enseignement qui y est donné, il en est renvoyé début 1831.

Ses activités politiques le conduisent en prison fin 1831. Après sa libération, il s'éprend en mai 1832 d'une femme, Stéphanie D., mais celle-ci semble le repousser. Quelques jours après il se bat en duel, probablement à cause de Stéphanie (« Je meurs pour une infâme coquette ») et peut-être aussi pour des raisons politiques. La nuit précédente il écrit la fameuse *lettre à Auguste Chevalier*, où il résume ses derniers travaux:

« Mon cher Ami, j'ai fait en analyse plusieurs choses nouvelles. Les unes concernent la théorie des Équations, les autres les fonctions Intégrales. Dans la théorie des équations, j'ai recherché lesquelles étaient résolubles par radicaux.... »

Il est grièvement blessé, et meurt le lendemain.

La théorie de Galois fait typiquement partie d'un cours de Master, et ne peut pas être expliquée en quelques lignes. Indiquons brièvement l'idée. Soit $P \in K[X]$ un polynôme de degré n, et soient $x_1, \ldots, x_n$ ses zéros dans un corps convenable. Galois lui associe un *groupe*, maintenant appelé le *groupe de Galois* de l'équation $P(x) = 0$: c'est le sous-groupe du groupe des permutations de $x_1, \ldots, x_n$ qui préserve toutes les relations algébriques entre les x_i (c'est-à-dire les relations de la forme $R(x_1, \ldots, x_n) = 0$ pour $R \in K[X_1, \ldots, X_n]$). Galois montre que ce groupe G contrôle complètement la structure de l'équation. Par exemple, celle-ci est résoluble par radicaux si et seulement si G possède la propriété suivante:

Il existe des sous-groupes $G_0 = \{1\} \subset G_1 \subset \ldots \subset G_r = G$, *et pour* $1 \leq i \leq r$ *un homomorphisme de* G_i *dans un groupe* commutatif A_i *tel que* $G_{i-1} = \operatorname{Ker} f_i$.

(On dit maintenant qu'un groupe vérifiant cette condition est *résoluble*; cela signifie que le groupe est proche d'être commutatif – il se construit à partir de "morceaux" commutatifs.)

Plus généralement, la connaissance du groupe de Galois de l'équation contient des informations profondes sur l'équation, par exemple sur les "équations réduites" (au sens de Lagrange) que peuvent vérifier certaines combinaisons des racines.

Le travail de Galois sur les équations est d'abord accueilli avec des réserves: les rapporteurs de l'Académie des Sciences affirment que le Mémoire est "à peu près inintelligible"; de plus ils se plaignent que la condition de résolubilité par radicaux n'est pas effective, et ne peut par exemple se décider au vu des coefficients de l'équation. Ce n'est qu'en 1846 que Liouville publie le "Mémoire sur les conditions de résolubilité des équations par radicaux", en insistant sur sa valeur:

« ... après avoir comblé de légères lacunes, j'ai reconnu l'exactitude entière de la méthode... »

Citant ensuite le cas particulier des équations de degré premier, Liouville écrit:

« Cette méthode, vraiment digne de l'attention des géomètres, suffirait seule pour assurer à notre compatriote un rang dans le petit nombre des savants qui ont mérité le titre d'inventeurs. »

Après cette publication, les travaux de Galois sont étudiés attentivement et leur importance est universellement reconnue; en particulier le "Traité des substitutions et des équations algébriques" de Jordan (1870, 667 pages) développe la théorie de Galois pratiquement jusqu'au point où elle est actuellement. On peut considérer que l'histoire des équations algébriques s'arrête là; ce qui continue, c'est le développement de la théorie de Galois, qui est encore aujourd'hui un sujet très riche – Laurent Lafforgue a obtenu en 2002 la médaille Fields, le prix Nobel des mathématiciens, pour ses travaux sur le *programme de Langlands*, un vaste ensemble de conjectures dans lequel le groupe de Galois joue un rôle essentiel.