La vie romantique d'Evariste Galois
Théorie de Galois : Résolubilité polynomiale

Hervé Stève
herve.steve@hotmail.fr

Kafemath du 29/11/2012

PLAN

1. Bio de Galois

2. Résolubilité des polynômes

3. Groupe de Galois

Bibliographie

- Caroline Ehrhardt « Evariste Galois ; la fabrication d'une icône mathématique » ed EHESS, 2011

- « Œuvres mathématiques d'Evariste Galois » Journal de math. Pures et appliquées, 1846, t11, p381-444

Évariste Galois

•Né le 25 oct 1811 à Bourg-la-Reine
•Mort le 31mai 1832 à Paris

•Bourgeoisie moyenne, lettrée
•Famille républicaine

•Collège Royal Louis-Le-Grand
jusqu'en « Maths Spé »
•Échoue 3 fois au concours de Polytechnique
•Rentre à l'École Préparatoire (Norm. Sup)

•Républicain militant (1830) : les Amis du Peuple
•Expulsion de l'École Préparatoire (déc 1830)
•Prison (1831-1832) à Sainte-Pélagie
•Duel le 30 mai 1832
•Fosse commune au cimetière Montparnasse

à 15 ans

Galois « matheux »

- Découvre les maths à 15 ans (1826)
  - « Éléments de géométrie » de Legendre
  - « Traités d'Algèbre et d'analyse » de Lagrange
  - Lauréat Concours Général en maths en 1827
  - Prépare concours de Polytechnique en solitaire
- En « maths spé » (1828-29) :
  - Publie un théorème sur les fractions continues
  - Envoie à l'académie des Sciences un mémoire sur les équations résolubles par radicaux

    (Cauchy / mémoires et commentaires perdus)

Galois chercheur

- Échec Prix de l'Académie des Sciences en 1830 : attribué à Abel et Jacobi
  - 2nd Mémoire perdu par Fourier qui est mort …
  - Grande déception de Galois
- 3 publications dans le bulletin de Férussac
- Crée un cours privé de mathématiques
- Recherche sur les fonctions elliptiques en 1831
- 3ème soumission à l'Académie des Sciences : Poisson
- « Testament » de mathématicien (veille du duel)
- Mémoire, papiers transmis à Joseph Liouville (École Polytechnique) : publication en 1846 dans le *Journal de mathématiques pures et appliquées*

Théorie de Galois

- Qu'est-ce qu'une théorie ?

Grec : observer, examiner

Sciences : modèle pour la compréhension de la nature et de l'humain

Maths : ensemble d'affirmations qui sont des axiomes et des théorèmes démontrables selon la logique

- théorie de Galois : étude des *extensions de corps* commutatifs, qui fait appel aux *groupes de Galois*
- Etude des équations algébriques qui se ramène à celle des *équations polynomiales*

$$p(x)=a_0+a_1x+a_2x^2+a_3x^3+a_4x^4+a_5x^5+\ldots a_nx^n=0$$

Résolubilité des polynômes

- Degré n : exposant le plus grand
- Solutions = racines, au plus n racines (théorème)
- Si racines connues (formule) alors p(x) est résolu
- Degré 1 : ax+b=0 => x=-b/a avec b non nul
- Degrés 2 à 4 : résolus depuis le 16ème
- Degré 5 et au delà ? Abel (1824) démontre l'impossibilité de la résolution par radicaux en faisant appel à l'étude des permutations des racines
- Galois innove en faisant intervenir une structure que l'on appellera « groupe » par la suite !

Second degré

$ax^2+bx+c=0$ avec a non nul

- Tablette babylonienne BM 13901 : 1700 a.j.c.
- Al Khwarizmi (9ème siècle) résolution systématique, formules *al-jabr* (algèbre)
- On simplifie : $x^2-sx+p=0$ avec $s=x_1+x_2$ et $p=x_1x_2$

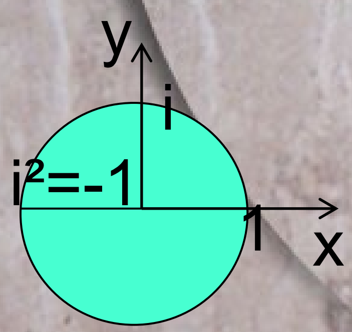
  Équivalent à $(x-s/2)^2 - (s^2/4-p) = 0$

  On pose $\Delta=s^2/4-p$ appelé *le discriminant*

  - Si $\Delta=0$ alors $x=x_1=x_2=s/2$: 1 racine double
  - Si $\Delta>0$ alors $x_1=s/2-\sqrt{\Delta}$ et $x_2=s/2+\sqrt{\Delta}$:

    2 racines réelles si a,b,c réels
  - Si $\Delta<0$ alors $x_1=s/2-i\sqrt{-\Delta}$ et $x_2=s/2+i\sqrt{-\Delta}$:

  2 racines complexes conjuguées si a,b,c réels



Troisième degré

$ax^3+bx^2+cx+d=0$ avec a non nul

- Méthode de Cardan (1545) empruntée à Tartaglia puis Euler (18ème) justifiera les solutions
- on pose $x=z-b/3a$, on se ramène à

$$z^3 + pz + q = 0$$

- soit $z=u+v$, on obtient le système à 2 équations :

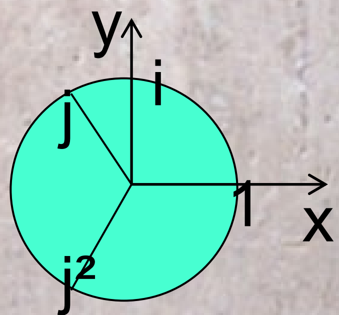
$$S=u^3+v^3=-q \text{ et } P=u^3v^3=-p^3/27$$

- alors $X=u^3$ ou v^3 solutions de

$$X^2+qX-p^3/27=0 \qquad \text{(degré 2)}$$

On a perdu un degré

Troisième degré (2)



- On obtient X_1, X_2 (cf degré 2)
- u, v racines cubiques de X_1, X_2
- 3 racines cubiques de 1 : $1, j, j^2$

  avec $j=-1/2+i\sqrt{3}/2$; $j^3=1$; $1+j+j^2=0$
- On a $z=u+v$ avec $uv=-p/3$
- On cherche $\alpha^3=u^3$ ou $\alpha'^3=u^3$ alors $u=j^{k-1}\alpha$ pour $k=1,2,3$

$$\alpha=\sqrt[3]{-\frac{q}{2}+\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}\,;\alpha'=\sqrt[3]{-\frac{q}{2}-\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}$$

- Trois solutions $z_k=j^{k-1}\alpha-p/(3j^{k-1}\alpha)$ pour $k=1,2,3$

  si on remplace α par α', on retrouve z_k

  cyclicité/permutation dans les racines

Troisième degré (3)

soit le discriminant $\Delta=q^2/4+p^3/27$

- Si $\Delta=0$ alors $X=u^3=v^3=-q/2$ soit $z_1=3q/p$, $z_2=z_3=-3q/2p$
  si p,q réels alors 2 solutions réelles

- Si $\Delta>0$ alors $u^3=-q/2-\sqrt{\Delta}$ et $v^3=-q/2+\sqrt{\Delta}$
  si p,q réels alors 1 solution réelle + 2 complexes conjuguées

- Si $\Delta<0$ alors $u^3=-q/2-i\sqrt{-\Delta}$ et $v^3=-q/2+i\sqrt{-\Delta}$
  si p,q réels alors 3 solutions réelles ! Trigonométrie

$$z_k=2\sqrt{\frac{-p}{3}}\cos\left(\frac{1}{3}\arccos\left(\frac{-q}{2}\sqrt{\frac{27}{-p^3}}\right)+\frac{2k\pi}{3}\right)\quad ;k=1,2,3$$

Nécessité de passer par les complexes pour trouver des solutions réelles !

quatrième degré

$ax^4+bx^3+cx^2+dx+e=0$ avec a non nul

- Résolu par Ferrari élève de Cardan
- Posons $x=y-b/4a$, alors on a $y^4+py^2+qy+r=0$
- Les 4 solutions sont de la forme $y=(\pm\sqrt{z_1}\pm\sqrt{z_2}\pm\sqrt{z_3})/2$

  avec z_1,z_2,z_3 vérifiant $\sqrt{z_1}\sqrt{z_2}\sqrt{z_3}=-q$

  et solutions de l'équation de degré 3 :

$$z^3+2pz^2+(p^2-4r)z-q^2=0$$

On a encore perdu un degré !

Degré 5 et plus

$$p(x)=a_0+a_1x+a_2x^2+a_3x^3+a_4x^4+a_5x^5+\ldots+a_nx^n$$

- Peut-on perdre encore un degré ? Voir Euler
- Les racines sont liées entre-elles par de permutations : voir Lagrange => Galois
- Certaines quintites sont résolubles à l'aide de radicaux …
- Sinon il reste la *résolution numérique* : par exemple avec la méthode itérative de Newton-Raphson

  x_0 non nul donné puis $x_{k+1}=x_k - p(x_k)/p'(x_k)$

  avec $p'(x)$ la dérivée de $p(x)$:

  $p'(x)= a_1+2a_2x+3a_3x^2+4a_4x^3+5a_5x^4+...na_nx^{n-1}$

  faire des essais avec différents x_0 , $p'(x_0)$ non nul

Groupe

un **groupe** est un ensemble muni d'une loi de composition interne associative admettant un élément neutre et, pour chaque élément de l'ensemble, un élément symétrique.

Exemple : les entiers relatifs Z muni de l'addition +

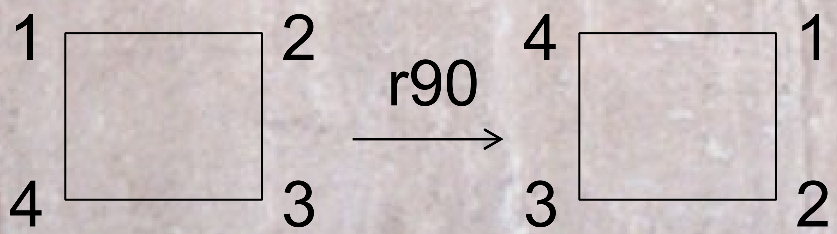
- si a,b dans Z alors a+b dans Z donc + loi de composition interne
- si a,b,c dans Z , on a (a+b)+c=a+(b+c) : associativité
- si a dans Z, a+0=0+a=a dans 0 est l'élément neutre
- Pour tout a dans Z, il existe b dans Z tq : a+b=b+a=0.
- L'élément b est noté –a élément symétrique de a ou opposé de a

(pour la multiplication x dans R : 1 est le neutre et 1/a est l'inverse de a : élément symétrique)

Groupe de symétrie

Exemple : les symétries D_4 avec les rotations et réflexions munies de la composition . qui laissent invariant un carré

La rotation de 90° vers la droite ; le retournement horizontal



$$\begin{matrix}12\\43\end{matrix} \xrightarrow{fh} \begin{matrix}43\\12\end{matrix}$$

D_4 : la transformation identique, neutre noté **id**, 3 rotations **r90, r180, r270**, 4 retournements vertical **fv**, horizontal **fh**, selon la première diagonale **fd1** et selon la seconde diagonale **fd2**. Loi interne (faire la table de Cayley)

Chaque élément a un élément symétrique (lui-même pour les retournements et r180; r270 pour r90)

Ce groupe n'est pas commutatif :

$$fh \,.\, r90 = fd2 \begin{matrix}32\\41\end{matrix} \neq r90 \,.\, fh = fd1 \begin{matrix}14\\23\end{matrix}$$

Groupe de Galois

le **groupe de Galois** d'une extension de corps *L* sur un corps *K* est le groupe des automorphismes de corps de *L* laissant *K* invariant

- Corps : c'est un ensemble muni de +, -, x et / : par exemple **R** ensemble des réels.
- Extension de corps : K est un corps L qui contient K comme sous-corps. Par exemple : **C** l'ensemble des nombre complexes est une extension de corps de **R**
- Un automorphisme est une bijection de K dans K qui préserve la structure de K (une symétrie). Les automorphismes de K forment un groupe.

Il s'agit d'appliquer les groupes de Galois aux polynômes p(x) sur un corps K, avec les permutations de ses racines pour obtenir (ou non) une condition de résolution par radicaux.

Applications

- **Equations algébriques …**
- **Théorie des corps** ou théorie de Galois

  sous-corps Z/pZ avec p premier
- **Théorie algébrique des nombres**

  nombres constructibles : polygones réguliers constructibles à la règle et au compas (théorème de Gauss-Wantzel) => pas de trisection de l'angle et duplication du cube
- **Géométrie algébrique**

  variétés algébriques : intersections de courbes, surfaces avec des équations polynômiales à plusieurs variables : $x^2+y^2=1$

  application : dernier théorème de Fermat $x^n+y^n=z^n$