



kafemath.fr

# Evariste Galois et Résolubilité polynomiale

Hervé Stève, ingénieur mathématicien  
cofondateur du KAFEMATH

herve.steve@hotmail.fr

Kafemath du 11/10/2024

LILLE



## Bienvenue sur le site de Kafemath !

Le [Kafemath](#) est un essai de café mathématique.  
Un café mathématique est aux mathématiques ce que le "café-philo" est à la philosophie !

### Années précédentes

[2024-2025](#)  
[2023-2024](#)  
[2022-2023](#)  
[2021-2022](#)  
[2020-2021](#)  
[2019-2020](#)  
[2018-2019](#)  
[2017-2018](#)  
[2016-2017](#)  
[2015-2016](#)  
[2014-2015](#)  
[2013-2014](#)  
[2012-2013](#)  
[2011-2012](#)  
[2010-2011](#)  
[2009-2010](#)  
[2008-2009](#)  
[2007-2008](#)  
[2006-2007](#)  
[2005-2006](#)  
[2004-2005](#)

**Les mathématiques sont un élément fondamental de la culture. Mais elles sont souvent trop isolées dans des lieux réservés aux spécialistes !**

**En veillant à rester ouvert à tous, au Kafemath, on parle de maths, on en découvre l'histoire, on en fait un peu, on en débat, on en apprend si on veut. On y rit et surtout, surtout, on y prend plaisir ! Ensemble.**

**Et il suffit d'être passionné pour devenir co-animateur !**



### Sites à visiter

[Catalogue  
2004-2023](#)





# PLAN

Biographie de Galois

Résolubilité des polynômes

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 31 mai 1832 à Paris à 20 ans !
- **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 (Normale 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 pour « une infâme coquette\* »  
Fosse commune au cimetière Montparnasse ?  
Cénotaphe dans le caveau familial à Bourg-la-Reine



à 15 ans



(\* ) Stéphanie Félicité Poterin du Motel



# Galois « matheux »

Découvre les maths à 15 ans (1826)

- « Éléments de géométrie » de **Legendre** 1752-1833
- « Traités d'Algèbre et d'analyse » de **Lagrange** 1736-1813
- 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**



**Louis Augustin Cauchy** 1789-1857 : jugé incompréhensible (mémoire et commentaires perdus)



# Galois chercheur



- Échec au Prix de l'Académie des Sciences en 1830 : attribué à **Niels Abel** 1802-1829 et **C. G. Jacobi** 1804-1851

2<sup>nd</sup> Mémoire perdu par **Joseph Fourier** 1768-1830 qui meurt : grande déception de Galois

- 3 publications dans le bulletin de Férussac
- Crée un cours privé de mathématiques
- Recherche sur les fonctions elliptiques en 1831
- 3<sup>ème</sup> soumission à l'Académie des Sciences : **S. D. Poisson** 1781-1840 ne juge pas utile le mémoire ...



- « Testament » de mathématicien (veille du duel)

Mémoire, papiers transmis en 1843 à **Joseph Liouville** 1809-1882 (École Polytechnique) : publication en 1846 dans le *Journal de mathématiques pures et appliquées*





# Théorie de Galois

- Qu'est-ce qu'une **théorie** ?

**Grec *theorein*** : 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*
- Étude des équations algébriques qui se ramène à celle des *équations polynomiales*

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



# Résolubilité des polynômes

- ◆ Degré  $n$  : exposant le plus grand
- ◆ **Théorème** : au plus  $n$  racines (ou solutions)
- ◆ Si racines connues (formules) alors  $p(x)$  est résolu
- ◆ Degré 1 :  $ax+b=0 \Rightarrow x=-b/a$  avec  $a$  non nul
- ◆ Degrés 2 à 4 : résolus depuis le 16ème
- ◆ Degré 5 et au delà ? **N. H. Abel** (1802-1829) démontre en 1824 l'impossibilité de la résolution par radicaux en faisant appel à l'étude des permutations des racines
- ◆ **E. Galois** innove en faisant intervenir une structure que l'on appellera « groupe » par la suite !





# Second degré

$$ax^2 + bx + c = 0 \text{ avec } a \text{ non nul}$$

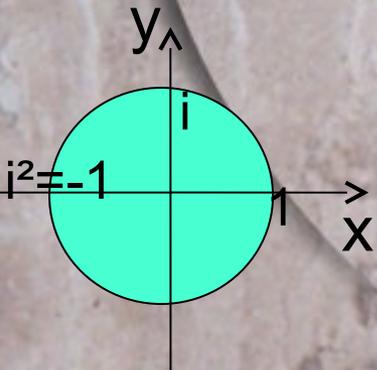
- Tablette babylonienne BM 13901 : 1700 a.j.c.
- **Al Khwarizmi** (9<sup>ème</sup> siècle) résolution systématique, formules *al-jabr* (algèbre)
- Soit  $x^2 - sx + p = 0$  avec  $s = x_1 + x_2 = -b/a$  et  $p = x_1 x_2 = c/a$

$$\text{alors on : } (x - s/2)^2 - (s^2/4 - p) = 0$$

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

- Si  $\Delta = 0$  alors  $x = x_1 = x_2 = s/2 = -b/2a$  : 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

$$ax^3 + bx^2 + cx + d = 0 \text{ avec } a \text{ non nul}$$



- 1545 : Méthode de [Girolamo Cardano](#) (1501-1576) empruntée à [Niccolo Fontana](#) (1499-1557) dit [Tartaglia](#) puis [Leonhard Euler](#) (1707-1783) 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 :

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

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

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

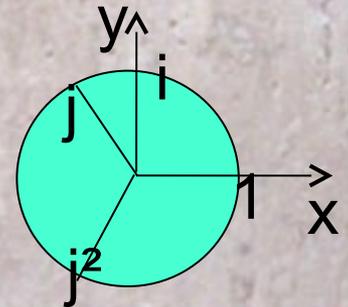
On a perdu un degré





# Troisième 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  $u = j^{k-1}\alpha$  et  $v = j^{k-1}\alpha'$  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  $z_1 = \alpha + \alpha'$  ;  $z_2 = j\alpha + j^2\alpha'$  ;  $z_3 = j^2\alpha + j\alpha'$

cyclicité/permutation des 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 3 solutions réelles dont 1 double
- 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  $z_1$  + 2 complexes conjuguées  $z_2, z_3$
- Si  $\Delta < 0$  alors  $u^3 = -q/2 - i\sqrt{-\Delta}$  et  $v^3 = -q/2 + i\sqrt{-\Delta}$

si  $p, q$  réels alors  $\alpha' = \text{conj}(\alpha)$  donc 3 solutions réelles !

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

**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 **Ludovico Ferrari** (1522-1565) élève de **Cardan**
- Méthode de **Joseph Louis Lagrange** (1735-1813) :



Posons  $x=y-b/4a$ , alors on a  $y^4+py^2+qy+r=0$

Soit  $y=(u+v+w)/2$ ;  $s=u^2+v^2+w^2$ ;  $t=u^2v^2+u^2w^2+w^2v^2$ ;  $g=uvw$

on obtient  $(y^2-s/4)^2=...=t/4 + gy$

donc  $y^4 - s/2 y^2 - gy + s^2/16 - t/4 = 0$

et  $p=-s/2$ ;  $q=-g$ ;  $r= s^2/16-t/4$  d'où  $t=p^2-4r$

soit  $X=[u^2,v^2,w^2]$  solutions de  $(X-u^2)(X-v^2)(X-w^2)=X^3-sX^2+tX-g^2=0$

et donc  $X^3 + 2pX^2 + (p^2-4r)X - q^2 = 0$  3<sup>ème</sup> degré  $\Rightarrow X$

Soit  $u=\pm\sqrt{X}$  alors  $v,w$  tq  $uvw=g=-q$ ,  $u^2+v^2+w^2=s=-2p$

on obtient les 4 sol  $y_1=(u+v+w)/2$ ;  $y_2=(u-v-w)/2$ ;

$y_3=(-u+v-w)/2$ ;  $y_4=(-u-v+w)/2$

On a encore perdu un degré !  
cyclicité/permutation des racines





# Degré 5 et plus

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

- Peut-on perdre encore un degré ? voir [Euler](#) ...
- Les racines sont-elles liées entre-elles par des permutations ? voir [Lagrange](#), [Abel](#) et [Galois](#)
- Certaines quintites sont résolubles à l'aide de radicaux ... ex)  $x^5 - 1 = 0 = (x - 1)(1 + x + x^2 + x^3 + x^4)$
- Sinon il reste la *résolution numérique* : par exemple avec la méthode itérative de [Newton-Raphson](#)



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

avec  $p'(x)$  la dérivée de  $p(x)$  :

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

faire des essais avec différents  $x_0$  ,  $p'(x_0)$  non nul 15



# Groupe

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  $\mathbf{Z}$  muni de l'addition +

- si  $a, b$  dans  $\mathbf{Z}$  alors  $a+b$  dans  $\mathbf{Z}$  donc + **loi de composition interne**
- si  $a, b, c$  dans  $\mathbf{Z}$ , on a  $(a+b)+c=a+(b+c)$  : **associativité**
- si  $a$  dans  $\mathbf{Z}$ ,  $a+0=0+a=a$  dans  $0$  est l'**élément neutre**
- Pour tout  $a$  dans  $\mathbf{Z}$ , il existe  $b$  dans  $\mathbf{Z}$  tq :  $a+b=b+a=0$ .

L'élément  $b$  est noté  $-a$  **élément symétrique** de  $a$  ou opposé de  $a$   
(pour la multiplication  $\times$  dans  $\mathbf{R}$  :  $1$  est le neutre et  $1/a$  est l'inverse de  $a$  : élément symétrique)

**Groupe commutatif ou abélien** :

si  $a, b$  dans  $\mathbf{Z}$  alors  $a+b=b+a$





# Groupes finis

- **Groupe cyclique abélien  $C_n = \mathbb{Z}/n\mathbb{Z} = \{0, 1, 2, \dots, n-1\}$  : ordre  $n$**   
Tout groupe abélien est produit de groupes cycliques (ex ordre 8 :  $C_8$  ;  $C_2 \times C_4$  ;  $C_2 \times C_2 \times C_2$ )
- **Groupe symétrique  $S_n$  permutations de  $n$  éléments : ordre  $n!$ \* ( $G_n$  Galois), non abélien  $n > 2$**
- **Groupe diédral  $D_n$  : ordre  $2n$ , isométrie plane**
- **Groupe des quaternions  $H_8$  : ordre 8,  $H_8 = C_2 \times D_2$**

$\{\pm 1, \pm i, \pm j, \pm k\}$  avec  $i^2 = j^2 = k^2 = -1$ ,  $ij = k$ ,  $jk = i$ ,  $ki = j$

$$1 \rightarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}; I \rightarrow \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}; J \rightarrow \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}; K \rightarrow \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

avec  $i^2 = -1$

(\*)  $n! = 1 \times 2 \times 3 \times \dots \times n$



# Groupes 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  $+$ ,  $-$ ,  $\times$  et  $/$  : par exemple  $\mathbf{R}$  ensemble des réels.
- **Extension de corps** : par exemple :  $\mathbf{C}$  l'ensemble des nombres complexes est une extension de corps de  $\mathbf{R}$
- Un **automorphisme** est une bijection de  $K$  dans  $L$  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  $\mathbf{R}$  ou  $\mathbf{C}$ , avec les permutations de ses racines pour obtenir (ou non) une condition de résolution par radicaux.



# Groupes de Galois (2)

$G_n$  **groupe de Galois** : permutations à  $n$  éléments d'ordre  $n!$ .

$A_n$  sous groupe de  $G_n$  des permutations paires\* d'ordre  $n!/2$  :

$$G_n = A_n \times C_2$$

(\*) permutations paires : nombre pair d'inversions

ex) paires : identité,  $n$ -cycles si  $n$  impair, ...

impaires :  $n$ -cycles si  $n$  pair, transpositions, ...

**Groupe résoluble :**

$G_n$  est résoluble si  $A_n$  est **sous groupe distingué**

$$\text{i.e } \forall y \in G_n, \forall x \in A_n \text{ alors } y x y^{-1} \in A_n$$

+ Tout sous groupe d'un groupe abélien est distingué, en particulier les groupes cycliques.

+ Le produit de groupes distingués est distingué.





# Théorème de Galois

$G_n$  est résoluble pour  $n < 5$

Démonstration :

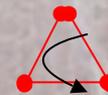
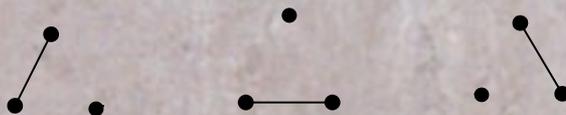
- $G_1 = \{\text{identité}\}$  groupe trivial

- $G_2 = \{\text{id}, \tau\} = C_2$  groupe cyclique  
avec  $\tau$  transposition =  $c_2$  2-cycle



- $G_3 = \{\text{id}, 3 \tau, 2 c_3\} = A_3 \times C_2$ , avec  $c_3$  3-cycle

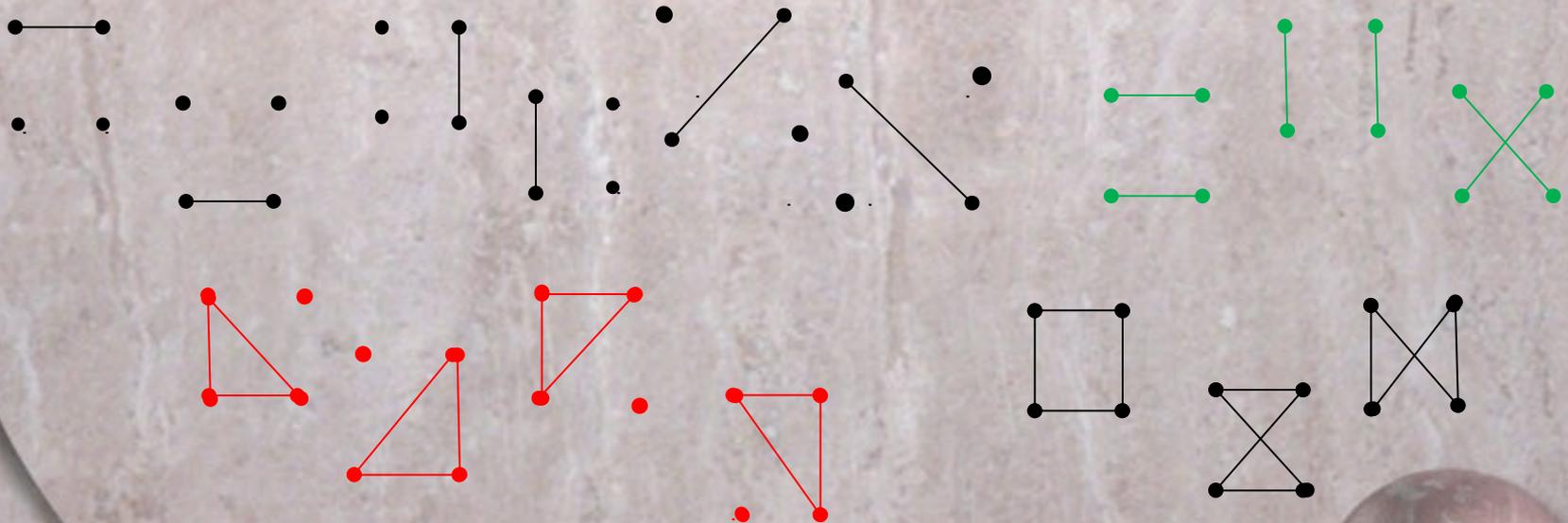
$A_3 = \{\text{id}, 2 c_3\} = C_3$  sous groupe distingué de  $G_3$





# G4 résoluble

- $G_4 = \{\text{id}, 6 \tau, 3 \tau', 8 c_3, 6 c_4\}$ , ordre 24 avec  $c_4$  4-cycle  
avec  $\tau' = \tau\tau$  bi transposition à support disjoint  
 $A_4 = \{\text{id}, 3 \tau', 8 c_3\}$  ordre 12 et  $V_4 = \{\text{id}, 3 \tau'\} = C_2 \times C_2$  ordre 4  
 $V_4$  groupe de Klein sous groupe distingué de  $A_4 = V_4 \times C_3$





# G5 non résoluble

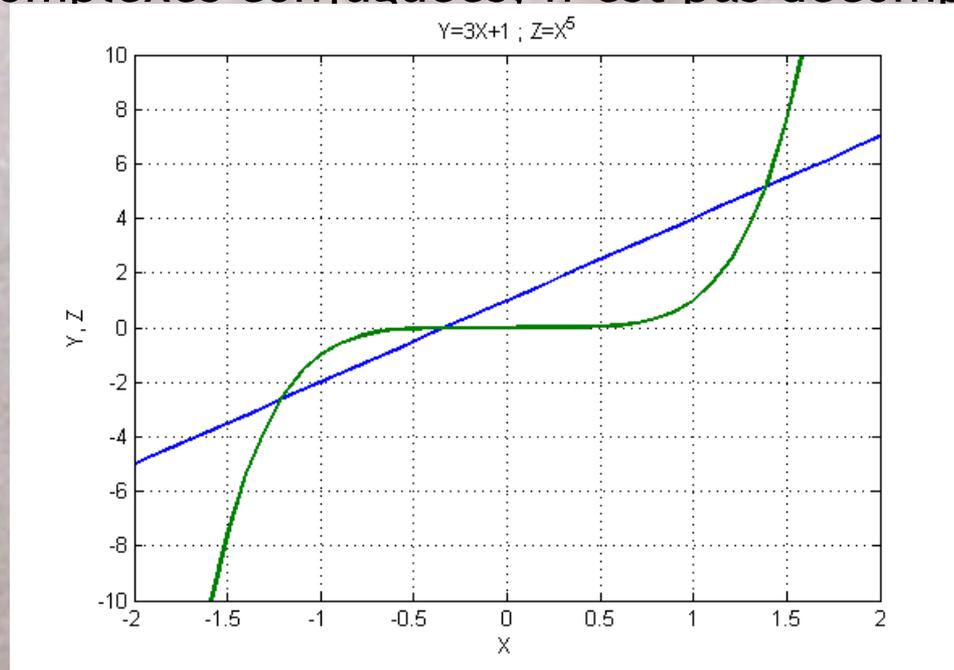
$G_5 = \{\text{id}, 10 \tau, 15 \tau', 20 c_3, 20 c_3\tau, 30 c_4, 24 c_5\}$  ordre 120

$A_5 = \{\text{id}, 15 \tau', 20 c_3, 24 c_5\}$  ordre 60 **n'est pas distingué !**

car  $1+15, 1+20, 1+24, 1+15+20, \dots$  ne divisent pas 60

Donc  $G_5$  n'est pas résoluble : CQFD

Exemple) le polynôme  $p(x) = x^5 - 3x - 1$  a 3 racines réelles et 2 complexes conjuguées, n'est pas décomposable...





# Applications

- **Équations algébriques ...**
- **Théorie des corps ou théorie de Galois**  
sous-corps  $C_p = \mathbb{Z}/p\mathbb{Z}$  avec  $p$  nombre 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 polynomiales à plusieurs variables :  
 $x^2 + y^2 = 1$   
  
=> dernier théorème de Pierre de Fermat (16?-1665):  
 $n > 2$ ,  $x^n + y^n = z^n$  n'a pas de solutions entières non triviales, prouvé par Andrew Wiles en 1994

