



WIKIPÉDIA  
L'encyclopédie libre

[Accueil](#)  
[Portails thématiques](#)  
[Article au hasard](#)  
[Contact](#)

[Contribuer](#)  
[Débuter sur Wikipédia](#)  
[Aide](#)  
[Communauté](#)  
[Modifications récentes](#)  
[Faire un don](#)

[Outils](#)  
[Pages liées](#)  
[Suivi des pages liées](#)  
[Importer un fichier](#)  
[Pages spéciales](#)  
[Lien permanent](#)  
[Informations sur la page](#)  
[Élément Wikidata](#)  
[Citer cette page](#)

[Imprimer / exporter](#)

[Créer un livre](#)  
[Télécharger comme PDF](#)  
[Version imprimable](#)

[Dans d'autres projets](#)



[Dans d'autres langues](#)



[العربية](#)  
[Deutsch](#)  
[English](#)  
[Español](#)  
[Italiano](#)  
[한국어](#)  
[Русский](#)  
[Tiếng Việt](#)  
[中文](#)

★A 24 de plus

[Modifier les liens](#)

Non connecté [Discussion](#) [Contributions](#) [Créer un compte](#) [Se connecter](#)

Article [Discussion](#)

Lire

[Modifier](#)

[Modifier le code](#)

Plus ▾

# Théorie de Galois

[\[masquer\]](#)

En [mathématiques](#) et plus précisément en [algèbre](#), la **théorie de Galois** est l'étude des [extensions](#) de [corps commutatifs](#), par le biais d'une correspondance avec des [groupes](#) de transformations sur ces extensions, les [groupes de Galois](#). Cette méthode féconde, qui constitue l'exemple historique, a essaimé dans bien d'autres branches des mathématiques, avec par exemple la [théorie de Galois différentielle](#), ou la théorie de Galois des [revêtements](#).

Cette théorie est née de l'étude par [Évariste Galois](#) des [équations algébriques](#). L'analyse de [permutations](#) des [racines](#) permet d'expliciter une condition nécessaire et suffisante de résolubilité par radicaux. Ce résultat est connu sous le nom de [théorème d'Abel-Ruffini](#).

Les applications sont très variées. Elles s'étendent de la résolution de vieilles conjectures comme la détermination des [polygones constructibles à la règle et au compas](#) démontrée par le [théorème de Gauss-Wantzel](#) à la [géométrie algébrique](#) à travers, par exemple, le [théorème des zéros de Hilbert](#).

## Sommaire [\[masquer\]](#)

- Histoire
  - Genèse
  - Gauss et les polynômes cyclotomiques
  - Théorème d'Abel-Ruffini
  - Évariste Galois
  - Structures algébriques
  - Théories de Galois
  - Apports du XX<sup>e</sup> siècle
- Exemples
  - Petit théorème de Fermat
  - Duplication du cube
  - Équation cubique
  - Synthèse
- Applications
  - Théorie algébrique des nombres
  - Cryptographie
  - Théorie des équations algébriques
  - Géométrie algébrique
- Les structures utilisées
  - Corps commutatifs
  - Espace vectoriel
  - Anneau
  - Groupe
  - Topologie
- Théories de Galois
  - Théorie classique

- 5.2 [Théorie de Galois infinie](#)
- 5.3 [Théorie géométrique](#)
- 5.4 [Théorie inverse](#)
- 5.5 [Théorie différentielle](#)
- 5.6 [Théorie des corps de classes](#)
- 6 [Notes et références](#)
- 7 [Voir aussi](#)
  - 7.1 [Bibliographie](#)
  - 7.2 [Liens externes](#)

## Histoire [ [modifier](#) | [modifier le code](#) ]

### Genèse [ [modifier](#) | [modifier le code](#) ]

La théorie de Galois voit ses origines dans l'étude des équations algébriques. Elle se ramène à l'analyse des équations polynomiales. Une approche par des changements de variables et des substitutions a permis à des mathématiciens comme [Al-Khwārizmī](#)<sup>1</sup> (783-850), [Tartaglia](#) (1499-1557), [Cardano](#)<sup>2</sup> (1501-1576) ou [Ferrari](#) (1522-1565) de résoudre tous les cas jusqu'au degré quatre. Cette approche ne permet pas d'aller plus loin et deux siècles seront nécessaires pour apporter de nouvelles idées.

### Gauss et les polynômes

#### cyclotomiques [ [modifier](#) | [modifier le code](#) ]

 Paragraphe détaillé : [Histoire des polynômes cyclotomiques](#).

[Gauss](#) utilise les [polynômes cyclotomiques](#)<sup>3</sup> pour apporter une contribution à un problème ouvert depuis l'antiquité : celui de la [construction à la règle et au compas](#) de [polygones réguliers](#). Il construit en particulier l'[heptadécagone](#), polygone régulier à dix-sept côtés. Son approche, typiquement galoisienne bien avant la découverte de la théorie, lui vaut le surnom de « prince des mathématiciens ».

Son travail est complété par [Wantzel](#)<sup>4</sup>, qui donne en 1837 une condition nécessaire et suffisante de constructibilité des polygones réguliers et démontre l'impossibilité de la [trisection de l'angle](#) et de la [duplication du cube](#).



Carl Friedrich Gauss  
(1777-1855).



### Théorème d'Abel-Ruffini [ [modifier](#) | [modifier le code](#) ]

 Paragraphe détaillé : [Histoire du théorème d'Abel-Ruffini](#).

Dans le cas général, l'[équation quintique](#) n'admet pas de solution par radicaux. C'est la raison pour laquelle une démarche à l'aide de substitutions et changements de variables devient stérile. [Lagrange](#)<sup>5</sup> (1736-1813) et [Vandermonde](#)<sup>6</sup> (1735-1796) utilisent la notion de permutation à la fin du XVIII<sup>e</sup> siècle et pressentent l'importance de cet outil dans le cadre de l'[équation polynomiale](#). [Ruffini](#)<sup>7</sup> (1765-1822) est le premier à prévoir l'impossibilité de la solution générale et que la compréhension du phénomène réside



Niels Abel (1802-1829).



dans l'étude des permutations des racines. Sa démonstration reste néanmoins peu rigoureuse et partielle. Le mathématicien norvégien [Abel](#) publie une démonstration<sup>8</sup> en 1824 qui finit par convaincre la communauté scientifique. Elle ne propose pas à l'époque de condition nécessaire et suffisante de résolubilité.

## Évariste Galois [ [modifier](#) | [modifier le code](#) ]

 Paragraphe détaillé : [Histoire des groupes de Galois](#).

En étudiant le problème de l'équation algébrique, [Galois](#) met en évidence les premiers éléments de la théorie qui porte maintenant son nom. Ses écrits sont perdus ou tombent dans l'oubli. Un mémoire<sup>9</sup> est finalement retrouvé par [Liouville](#) (1809-1882) qui le présente à l'[Académie des sciences](#) en 1843. Les travaux de Galois accèdent alors *in extremis* à la célébrité.

Galois met en évidence la correspondance univoque des [sous-corps](#) d'une [extension finie](#), avec les [sous-groupes](#) d'un certain [groupe de permutations](#) qu'il associe à cette extension, appelé aujourd'hui [groupe de Galois](#). L'étude des propriétés des extensions finies se ramène alors à l'étude de leur groupe de Galois. Armé de cet instrument profondément novateur et puissant, Galois est en mesure de donner une condition nécessaire et suffisante pour la résolution d'une équation algébrique au moyen de radicaux. Il emploie ensuite sa théorie pour établir des théorèmes particuliers sur certaines équations algébriques : par exemple, il démontre (fait énoncé sans preuve par Abel) que pour qu'une équation de degré [premier](#) soit résoluble par radicaux, il faut et il suffit que toutes ses racines soient fonctions rationnelles de deux d'entre elles. De même, il démontre que l'équation générale de degré supérieur à 4 ne peut être résolue par radicaux. Pour ces démonstrations, Galois utilise intensivement la [structure de groupe](#), introduite par Lagrange, Cauchy, Ruffini et Abel dans la [théorie des équations](#) (comme pour ses prédécesseurs, les groupes envisagés par Galois ne sont pas des groupes abstraits, définis par un ensemble et une loi, mais des groupes de permutations). De plus, pour obtenir des indices qui varient d'une certaine manière, Galois est conduit à inventer la théorie des [corps finis](#), et à en développer à peu près toutes les propriétés élémentaires classiques. De la sorte, il peut faire varier les indices des variables dans des corps finis, et étudier des équations particulières qu'il nomme « primitives ».

La démarche [fonctorielle](#) de Galois, particulièrement novatrice, est à l'origine de l'algèbre moderne <sup>[[source insuffisante](#)]</sup>. [Liouville](#) en parle dans les termes suivants : « 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'inventeur<sup>10</sup>. »

## Structures algébriques [ [modifier](#) | [modifier le code](#) ]

 Article détaillé : [Théorie de Galois à l'origine](#).

La notion de groupe est issue de la théorie des substitutions pour la résolution des équations algébriques, à laquelle ont contribué [Joseph-Louis Lagrange](#), [Alexandre-Théophile Vandermonde](#), [Carl Friedrich Gauss](#), [Paolo Ruffini](#), [Niels Henrik Abel](#) et [Augustin Louis Cauchy](#). Ce dernier considère un « ensemble » de permutations d'un « ensemble » fini (les notions ensemblistes ne sont pas encore connues, c'est pourquoi les guillemets s'imposent), muni de la composition des applications, et dégage les propriétés de cette loi interne (élément neutre, transitivité, éléments permutable, etc.). Il publie vingt-cinq articles sur les « groupes » (dans la terminologie actuelle)



Évariste Galois (1811-1832).

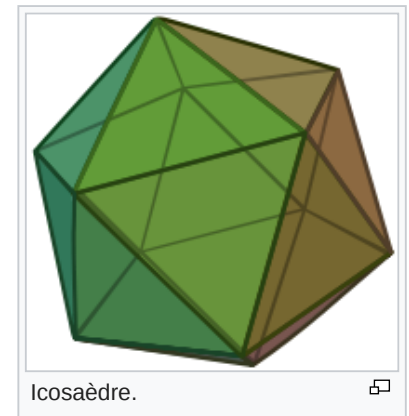


dont un sur [son célèbre théorème](#)<sup>11</sup>. Mais l'apport majeur est dû à Galois, lequel est le premier à dégager la notion de [sous-groupe distingué](#)<sup>12</sup> et à qui revient la première idée de la notion de représentation linéaire d'un groupe<sup>13</sup>. C'est également sous sa plume qu'apparaît le terme *groupe* d'une équation algébrique<sup>14</sup>. Après la publication de ses travaux par [Joseph Liouville](#) en 1846, ceux-ci ont commencé à être compris par la communauté mathématique. [Cayley](#) parvient en 1854 à la notion d'un groupe abstrait<sup>15</sup>, dont la première définition claire est donnée par [Walther Dyck](#) en 1882<sup>16</sup>. En 1869, dans un article paru dans les *Mathematische Annalen*<sup>17</sup>, puis, avec de légères modifications, dans son livre<sup>18</sup> publié en 1870, [Jordan](#) diffuse largement les idées de Galois et donne une caractérisation plus maniable que celle de Galois de la notion de groupe résoluble<sup>19</sup>. En 1893, [Weber](#) fait un exposé synthétique de la théorie des groupes<sup>20</sup>.

D'autres structures sont mises en évidence, particulièrement en Allemagne. Indépendamment des travaux de Galois, [Kummer](#) étudie<sup>21</sup> des [anneaux](#) et découvre l'ancêtre de la notion d'[idéal](#). [Kronecker](#) et [Dedekind](#) développent les prémisses de la théorie des anneaux et des corps<sup>22</sup>. Kronecker établit le pont entre les écoles française et allemande. Il donne la définition moderne de groupe de Galois à partir d'[automorphismes de corps](#).

## Théories de Galois [ [modifier](#) | [modifier le code](#) ]

Un nouvel axe d'analyse enrichit la théorie de Galois. En 1872, [Klein \(1849-1925\)](#) se fixe comme objectif de classifier les différentes [géométries](#) de l'époque. Il dégage, dans son célèbre [programme d'Erlangen](#), le principe général qu'une géométrie est définie par un espace et un groupe opérant sur cet espace, appelé groupe des [isométries](#). Un pont est ainsi établi entre la théorie des groupes et la géométrie. Ces premiers groupes correspondent à des [groupes de Lie](#) et n'appartiennent pas directement à ceux de la théorie de Galois.



En 1884, [Klein](#) remarque<sup>23</sup> que le groupe des isométries laissant invariant l'[icosaèdre](#) est isomorphe au groupe de Galois d'une équation quintique. La théorie de Galois s'étend à la [géométrie algébrique](#). Les groupes de Galois prennent alors la forme de [revêtements](#) aussi appelés revêtement de Galois. [Hilbert \(1862-1943\)](#) étudie les corps de nombres quadratiques et apporte une contribution majeure à la théorie en démontrant<sup>24</sup> son célèbre [théorème des zéros](#). Ce théorème possède aussi une interprétation géométrique sur les [variétés algébriques](#). La théorie est maintenant enrichie d'une nouvelle branche : la théorie de Galois géométrique, qui s'avère particulièrement féconde.

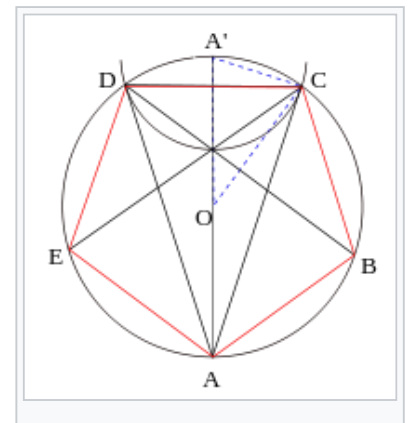
Les travaux de Hilbert ouvrent d'autres branches de la théorie de Galois. Le théorème des zéros permet l'étude des premiers groupes de Galois infinis. Son théorème d'irréductibilité ouvre [la problématique inverse](#). Elle s'énonce de la manière suivante : si  $G$  est un groupe alors est-il le groupe de Galois d'une extension ?

Enfin les travaux de [Picard \(1856-1941\)](#) et [Vessiot \(1865-1952\)](#) ouvrent une autre voie pour l'étude des groupes de Galois infinis, la [théorie de Galois différentielle](#).

## Apports du xx<sup>e</sup> siècle [ [modifier](#) | [modifier le code](#) ]

Les travaux de Hilbert ont ouvert l'étude des cas où le groupe de Galois est infini et commutatif. Ce vaste sujet prend le nom de [théorie des corps de classes](#). Elle est maintenant achevée et est souvent considérée comme un des plus beaux succès des mathématiques du xx<sup>e</sup> siècle.

La théorie de Galois a maintenant des ramifications importantes en géométrie algébrique. Elle est la base d'une quantité majeure des grandes réalisations mathématiques du  $xx^e$  siècle. L'alliance de la géométrie et de l'algèbre est presque systématiquement utilisée. On peut citer par exemple les travaux des mathématiciens [Jean-Pierre Serre](#) (*Médaille Fields* 1954) et [Grothendieck](#) (*Médaille Fields* 1966) avec une refonte de la géométrie algébrique, [Faltings](#) (*Médaille Fields* 1986) pour ses travaux sur les [modules](#) de Galois démontrant la [conjecture de Mordell](#) ou [Laurent Lafforgue](#) (*Médaille Fields* 2002) sur le [programme de Langlands](#), une généralisation de la théorie des corps de classes.



des [rationnels](#) — c'est-à-dire une extension de  $\mathbb{Q}$  de degré 2 — soit dans une extension quadratique d'un tel corps, et ainsi de suite. On parle alors de [tour d'extensions](#)

[quadratiques](#). On en déduit — cf. « [Conséquences du théorème de Wantzel](#) » — que tout nombre constructible est [algébrique](#) et que le degré de son [polynôme minimal](#) est une puissance de 2.

Puisque  $\sqrt[3]{2}$  a pour polynôme minimal  $X^3 - 2$ , il n'est donc pas constructible, ce qui prouve l'impossibilité de la duplication du cube.

Une construction du [pentagone régulier](#) à la règle et au compas.

## Équation cubique [ [modifier](#) | [modifier le code](#) ]

 Paragraphe détaillé : [Le cas du degré trois dans le théorème d'Abel](#).

Considérons un exemple d'[équation du troisième degré](#) :

$$P(X) = 0 \quad \text{avec} \quad P(X) = X^3 - 3X + 1.$$

Le polynôme  $P$  est un [polynôme irréductible](#) à [coefficients](#) rationnels 1, 0,  $p = -3$  et  $q = 1$ . On obtient

$$-4p^3 - 27q^2 = \delta^2 \quad \text{pour} \quad \delta = 9 \in \mathbb{Q}.$$

La théorie de Galois nous indique (cf. [article détaillé](#)) que dans ce cas :

- le [corps de décomposition](#)  $L$  de  $P$  a pour groupe de Galois  $A_3$  ;
- c'est une extension de  $\mathbb{Q}$  de degré 3 ;
- en diagonalisant un générateur du groupe de Galois, on montre de plus que les racines de  $P$  sont de la forme

$$u + v, \quad ju + j^2v \quad \text{et} \quad j^2u + jv$$

avec

$$uv = -\frac{p}{3} = 1 \quad \text{et} \quad u^3 + v^3 = -q = -1.$$

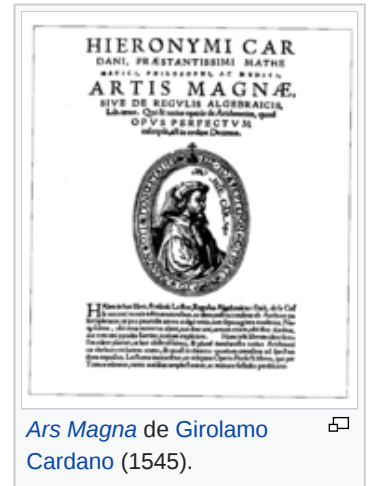
On en déduit que  $u^3$  et  $v^3$  vérifient l'équation  $X^2 + X + 1 = 0$ , ce qui permet de conclure que les racines de  $P$  sont  $2 \cos(2\pi/9)$ ,  $2 \cos(8\pi/9)$  et  $2 \cos(14\pi/9)$ .

Le groupe de Galois permet la résolution de l'équation cubique par une [diagonalisation](#) d'un [endomorphisme](#). La méthode est généralisable si et seulement si le groupe de Galois possède de bonnes propriétés, en fait s'il est [résoluble](#).

## Synthèse [ [modifier](#) | [modifier le code](#) ]

Ces exemples ont un point commun, ce sont les propriétés des structures algébriques qui permettent de trouver les solutions. Pour le premier exemple, la propriété démontrée par Lagrange sur les groupes (et donc les groupes multiplicatifs des corps) finis permet de conclure. Dans le deuxième exemple, ce sont les propriétés associées sur la [dimension d'un espace vectoriel](#) qui sont utilisées. Dans le troisième cas, sont utilisées les propriétés des corps et de leurs extensions, des groupes avec le théorème de Lagrange et celle des espaces vectoriels avec les propriétés de [réduction d'endomorphisme](#) dans le cas où le [polynôme minimal](#) est scindé.

La théorie de Galois offre une richesse dans les structures algébriques permettant de résoudre nombre de cas très différents et dans des domaines éloignés.



[Ars Magna](#) de Girolamo Cardano (1545).



## Applications [ [modifier](#) | [modifier le code](#) ]

### Théorie algébrique des nombres [ [modifier](#) | [modifier le code](#) ]

La [théorie algébrique des nombres](#) est l'étude des nombres racines d'un polynôme à coefficients entiers, appelés [nombres algébriques](#).

La théorie de Galois est ici essentielle car elle offre la structure la plus adéquate d'analyse, à savoir l'[extension finie](#) la plus petite contenant les nombres étudiés. Un sous-ensemble joue un rôle particulier : celui des [entiers algébriques](#), ils correspondent à la généralisation des entiers dans l'extension. L'étude de cet ensemble ajoute à la théorie de Galois de nombreuses propriétés issues de la théorie des anneaux. Les entiers algébriques jouent un rôle important pour la résolution d'équations d'[arithmétique modulaire](#) ou [diophantiennes](#).

On peut citer comme application de la théorie de Galois à ce domaine, le [théorème de Gauss-Wantzel](#) qui détermine tous les polygones réguliers constructibles à la règle et au compas. La [théorie de Kummer](#) s'applique aux équations diophantiennes et permet de valider le [grand théorème de Fermat](#) pour presque tous les entiers inférieurs à cent. Enfin, dans le cadre de l'arithmétique modulaire, la [loi de réciprocité d'Artin](#) généralise la [loi de réciprocité quadratique](#) de Gauss et résout le neuvième [problème de Hilbert](#).

### Cryptographie [ [modifier](#) | [modifier le code](#) ]

La [cryptographie](#) est la discipline qui s'attache à protéger un message. Le cadre théorique maintenant le plus utilisé consiste à définir un [algorithme](#) qui, associé à une clef permet de créer un nouveau message dit [cryptogramme](#) signifiant qu'il est chiffré. Le message chiffré est simple à déchiffrer, c'est-à-dire simple à transformer en message d'origine avec une clef et difficile sans celle-ci pour la personne qui s'efforce alors de le décrypter.

Dans une partie des théories modernes de cryptographie, les lettres du message sont choisies dans un corps fini. Le cadre est donc celui de la théorie de Galois [[réf. nécessaire](#)].

Il est naturel que les outils associés soient ceux de la théorie. L'arithmétique modulaire (cf. par exemple l'algorithme [RSA](#)) est très largement employée. Si les techniques simples reposent sur des résultats élémentaires comme le [théorème de Bézout](#), le [théorème des restes chinois](#) ou l'[exponentiation modulaire](#), les développements actuels utilisent des outils plus subtils comme les courbes elliptiques (cf. [Une clé privée inviolable ?](#)).


### Théorie des équations algébriques [ [modifier](#) | [modifier le code](#) ]

La problématique de la théorie des équations algébriques est celle qui donna naissance à la théorie de Galois. Elle complète le [théorème d'Abel-Ruffini](#) en proposant une condition nécessaire et suffisante pour l'existence d'une expression par radicaux des racines d'un polynôme.

Elle permet néanmoins d'aller plus loin. Le [théorème de Kronecker-Weber](#) explicite précisément la structure des extensions rationnelles associées aux polynômes ayant des racines s'exprimant par radicaux. Il devient alors possible de résoudre explicitement *toutes* les équations de cette nature.

Elle possède pour champs d'application tous les corps, offrant un outil puissant à l'[arithmétique modulaire](#). Beaucoup de lois de réciprocité, de même nature que celle démontrée par Gauss dans



La machine *Lorenz* utilisée par les Allemands durant la [Seconde Guerre mondiale](#). 

le cas quadratique sont ainsi démontrables grâce à la théorie de Galois.

Abel puis [Hermite \(1822-1902\)](#) ont travaillé sur une autre approche : les [fonctions elliptiques](#). Elles permettent, par exemple, d'exprimer les racines de toute équation polynomiale. La théorie géométrique de Galois intègre cette notion à travers les [courbes elliptiques](#). Le [grand théorème de Fermat](#) a été démontré à l'aide de méthodes de cette nature.

Il existe une théorie de Galois un peu particulière traitant des [équations différentielles](#) polynomiales. Cette théorie prend le nom de [théorie de Galois différentielle](#). Elle étudie une famille particulière d'extensions de corps appelées extensions de [corps différentiels](#). Ces extensions possèdent des groupes de Galois. La résolution d'une équation algébrique correspond aussi à l'analyse du groupe associé et permet la résolution d'une équation différentielle.

## Géométrie algébrique [ [modifier](#) | [modifier le code](#) ]

 Cette section est vide, insuffisamment détaillée ou incomplète. [Votre aide](#) est la bienvenue !  
[Comment faire ?](#)

 Article détaillé : [Géométrie algébrique](#).

## Les structures utilisées [ [modifier](#) | [modifier le code](#) ]

### Corps commutatifs [ [modifier](#) | [modifier le code](#) ]

 Articles détaillés : [Corps commutatif](#) et [Extension de corps](#).

Le corps commutatif est l'objet de la théorie de Galois. C'est donc naturellement la structure centrale de la théorie.

La technique la plus importante de construction correspond à l'[extension](#), c'est-à-dire à un corps qui contient le corps d'origine. À partir d'un corps de base, souvent le plus petit, celui engendré par l'unité, qui est un corps cyclique (construit à partir d'un [groupe cyclique](#) d'ordre un nombre premier) ou celui des [rationnels](#) une nouvelle structure est créée.

Cette méthode permet la création d'une « zoologie » décrivant les différentes propriétés de la structure. Un corps peut ainsi être par exemple [algébrique](#), [simple](#), [parfait](#), [quadratique](#), [séparable](#), [cyclotomique](#) ou [algébriquement clos](#).

Il existe des théorèmes importants, comme [celui de l'élément primitif](#) ou [celui de Wedderburn](#), qui assure que tout corps fini est commutatif.

### Espace vectoriel [ [modifier](#) | [modifier le code](#) ]

 Article détaillé : [Extension finie](#).

Une extension possède une structure d'[espace vectoriel](#) sur son corps de base. Cette structure est importante à deux titres :

- elle permet de classer l'étude des différents corps, le cas le plus simple étant celui des extensions finies ;
- elle est ensuite un outil qui permet la démonstration de nombreuses propriétés en adjoignant à la théorie les théorèmes d'algèbres linéaires. On peut citer par exemple le [théorème de Gauss-Wantzel](#) dont la démonstration se trouve dans le [paragraphe « Applications »](#) de l'article sur les tours d'extensions quadratiques ou le [théorème d'Abel-Ruffini](#) qui utilise une diagonalisation d'endomorphisme.



Le cas de dimension infinie est largement plus complexe ; il est partiellement traité dans la [théorie des corps de classes](#).

## Anneau [ [modifier](#) | [modifier le code](#) ]

 Article détaillé : [Extension algébrique](#).

Un outil important de la théorie est le [polynôme formel](#). Et la structure d'anneau est celle de l'[ensemble des polynômes](#). Il est utilisé par exemple pour construire des extensions. Une extension est ainsi souvent le quotient de l'anneau des polynômes par un [idéal](#) engendré par un polynôme irréductible.

Un polynôme joue un rôle particulier dans la théorie : le [polynôme minimal](#) qui est le polynôme unitaire de plus petit degré qui possède pour [racine](#) un élément donné. Ainsi, une extension est algébrique si tous les éléments possèdent un polynôme minimal, quadratique si le polynôme minimal de tout élément est de degré inférieur ou égal à deux, séparable si aucun polynôme minimal n'a de racine multiple, [cyclotomique](#) si l'extension est engendrée par une racine d'un [polynôme cyclotomique](#). Un corps est parfait si toute extension est séparable.

La théorie algébrique des nombres utilise aussi souvent des sous-ensembles d'une extension ne disposant que d'une structure d'anneau, comme les [entiers algébriques](#).

## Groupe [ [modifier](#) | [modifier le code](#) ]

 Articles détaillés : [Groupe de Galois](#) et [Théorème fondamental de la théorie de Galois](#).

Cette structure est l'apport majeur de Galois.

Le groupe de Galois est le groupe des [automorphismes d'une extension](#) laissant invariant le corps de base. Sous certaines conditions relativement générales, le corps est entièrement caractérisé par son groupe de Galois. Une extension satisfaisant ces conditions est dite [galoisienne](#). En particulier, si la structure d'espace vectoriel est de dimension finie, alors le groupe d'une extension abélienne a pour ordre la dimension du groupe.

Comme il est largement plus simple d'étudier un groupe fini qu'une structure de corps, l'analyse du groupe est une puissante méthode pour comprendre le corps. Le groupe de Galois est à l'origine de nombreux théorèmes. On peut citer le théorème fondamental de la théorie, le théorème d'Abel-Ruffini ou [celui de Kronecker-Weber](#).

## Topologie [ [modifier](#) | [modifier le code](#) ]

 Cette section est vide, insuffisamment détaillée ou incomplète. [Votre aide](#) est la bienvenue !  
[Comment faire ?](#)

## Théories de Galois [ [modifier](#) | [modifier le code](#) ]

### Théorie classique [ [modifier](#) | [modifier le code](#) ]

Le terme de *classique* est largement utilisé, même s'il ne possède pas de définition précise. On le trouve, par exemple, sur la page de présentation d'un membre de l'[Académie des sciences](#) : [Jean-Pierre Ramis](#).

Il désigne en général la théorie recouvrant les [extensions algébriques finies](#) et [séparables](#). La théorie traite essentiellement des [extensions normales](#) et donc [galoisiennes](#). Les résultats principaux sont le [théorème de l'élément primitif](#) et le [théorème fondamental de la théorie de](#)

**Galois**. Ce cadre permet par exemple la démonstration des théorèmes [d'Abel-Ruffini](#), [de Gauss-Wantzel](#) ou [de Kronecker-Weber](#) ; il est utilisé dans la classification des [corps finis](#).

L'étendue de cette théorie couvre l'état de la science à l'époque de Weber, c'est-à-dire la fin du  $\text{xix}^{\text{e}}$  siècle, même si maintenant elle est très généralement présentée avec le formalisme d'Artin. Cela correspond un peu au cas de la dimension finie pour l'algèbre linéaire.

## Théorie de Galois infinie [\[ modifier | modifier le code \]](#)

La théorie de Galois classique traite le cas des extensions algébriques finies. Toutefois, elle ne s'avère pas assez puissante pour traiter aussi celui des extensions algébriques infinies. Pour cela une étude algébrique ne s'avère pas suffisante, il faut y ajouter l'utilisation de propriétés [topologiques](#).

Une extension algébrique est dite [galoisienne](#) si elle est [séparable](#) et [normale](#). Son groupe de Galois peut alors être défini comme dans le cas classique, mais on y ajoute une topologie qui en fait un [groupe topologique compact](#). Dans le cas d'une extension finie, cette topologie est [discrète](#), de sorte que la seule information contenue dans le groupe de Galois est de nature algébrique.

Dans ce cadre, il existe un analogue au théorème fondamental de la théorie de Galois, qui donne une correspondance entre les sous-groupes fermés du groupe de Galois et les extensions intermédiaires de corps.

## Théorie géométrique [\[ modifier | modifier le code \]](#)

 Cette section est vide, insuffisamment détaillée ou incomplète. [Votre aide](#) est la bienvenue !  
[Comment faire ?](#)

## Théorie inverse [\[ modifier | modifier le code \]](#)

 Article détaillé : [Théorie de Galois inverse](#).

Il est en général difficile de déterminer le groupe de Galois d'une extension donnée, mais la question réciproque est tout aussi intéressante : soit un groupe fini, y a-t-il une extension galoisienne du corps  $\mathbb{Q}$  des rationnels qui possède ce groupe comme groupe de Galois ? C'est à cette question, et ses généralisations à d'autres groupes ou d'autres corps, que la théorie inverse cherche à répondre.

Dans le cas des groupes finis, un premier résultat montre que si  $n$  est un entier strictement positif alors il existe une extension de  $\mathbb{Q}$  ayant pour groupe de Galois le [groupe symétrique](#) d'ordre  $n$  (par exemple, le [corps de décomposition](#) du polynôme rationnel  $X^n - X - 1$  convient). Un [corollaire](#) marginal mais [immédiat](#) est que pour tout groupe fini  $G$ , il existe au moins un [corps de nombres](#) (c'est-à-dire une [extension finie](#) de  $\mathbb{Q}$ ) et une extension galoisienne de ce corps ayant  $G$  pour groupe de Galois.

De façon plus précise la théorie inverse cherche à répondre à deux questions :

- Soit un groupe fini (ou [profini](#)) et un corps, existe-t-il une extension galoisienne de ce corps ayant pour groupe de Galois ce groupe ?
- Soit un groupe fini (ou profini), existe-t-il une extension galoisienne de  $\mathbb{Q}$  ayant pour groupe de Galois ce groupe ?

Malgré d'importants progrès durant les trente dernières années du  $\text{xx}^{\text{e}}$  siècle, ces questions restent très largement ouvertes.

## Théorie différentielle [ [modifier](#) | [modifier le code](#) ]

La plupart des fonctions obtenues par addition, multiplication, division et composition de fonctions élémentaires (polynômes, exponentielle et logarithme par exemple) n'admettent aucune [primitive](#) qui puisse s'obtenir de la même manière ; c'est le cas par exemple de la [fonction gaussienne](#) d'expression  $x \mapsto \exp(-x^2/2)$ . Ce résultat, et la forme exacte des fonctions admettant une telle primitive, sont donnés par le [théorème de Liouville](#).

Ce théorème est généralisé par la [théorie de Galois différentielle](#), qui permet de déterminer, dans un ensemble d'équations différentielles dont les coefficients sont des fonctions d'une classe donnée, celles qui admettent une solution de la même classe. Cette théorie étudie des corps particuliers appelés [corps différentiels](#). Ce sont les corps  $K$  munis d'une [dérivation](#), c'est-à-dire d'une application  $\delta$  vérifiant la propriété suivante :

$$\forall a, b \in K \quad \delta(a + b) = \delta(a) + \delta(b) \quad \text{et} \quad \delta(ab) = \delta(a)b + a\delta(b).$$

Cette branche traite d'une famille de corps dotés d'une structure supplémentaire ; il est donc naturel de la considérer comme une variante de la théorie de Galois. Cependant l'analogie va plus loin et à bien des égards, cette théorie ressemble à la théorie classique. La différence principale est que, dans ce contexte, le groupe de Galois n'est plus un groupe fini mais en général un [groupe algébrique](#).

## Théorie des corps de classes [ [modifier](#) | [modifier le code](#) ]

 Article détaillé : [Théorie des corps de classes](#).

## Notes et références [ [modifier](#) | [modifier le code](#) ]

- ↑ Al-Khwārizmī, *Abrégé du calcul par la restauration et la comparaison*.
- ↑ **(1a)** Girolamo Cardano, *Ars Magna*, 1554.
- ↑ **(1a)** Carl Friedrich Gauss, *Disquisitiones arithmeticae*, 1801.
- ↑ Voir les articles « [Théorème de Wantzel](#) » et « [Théorème de Gauss-Wantzel](#) ».
- ↑ Joseph-Louis Lagrange, *Réflexions sur la résolution algébrique des équations*, 1770.
- ↑ Alexandre-Théophile Vandermonde, *Mémoire sur la résolution des équations*, 1771.
- ↑ **(1t)** P. Ruffini, *Teoria Generale delle Equazioni, in cui si dimostra impossibile la soluzione algebrica delle equazioni generali di grado superiore al quarto*, 1799.
- ↑ Niels Henrik Abel, *Mémoire sur les équations algébriques, où l'on démontre l'impossibilité de la résolution de l'équation générale du cinquième degré*, 1824.
- ↑ Évariste Galois, *Mémoire sur les conditions de résolubilité des équations par radicaux*, texte manuscrit de 1830, publié en 1846 au [Journal de mathématiques pures et appliquées, en ligne](#)<sup>[[archive](#)]</sup> sur le site [bibnum](#) avec une analyse par Caroline Ehrhardt.
- ↑ Joseph Liouville, « Œuvres Mathématiques d'Évariste Galois, suivies d'un avertissement de Liouville », *Journal de mathématiques pures et appliquées*, vol. XI, 1846.
- ↑ Augustin Louis Cauchy, « Sur le nombre de valeurs égales ou inégales que peut acquérir une fonction de  $n$  variables indépendantes, quand on permute ces variables entre elles d'une manière quelconque », *C. R.*, t. XXI, p. 593 (15 septembre 1845), [lire en ligne]<sup>[[archive](#)]</sup>.
- ↑ **(en)** Hans Wussing **(en)**, *The Genesis of the Abstract Group Concept*, 1984, réimpr. Dover 2007, p. 105.
- ↑ N. Bourbaki, *Algèbre*, Hermann, 1970, chap. I, p. 162.
- ↑ Jean Dieudonné, *Abrégé d'histoire des mathématiques*, Hermann, 1978, p. 77.
- ↑ **(en)** Arthur Cayley, « On the theory of groups, as depending on the symbolic equation  $\theta^n=1$  », *Philos. Mag.*, vol. 7, n<sup>o</sup> 4, 1854, p. 40-47.
- ↑ **(de)** Walther Dyck, « Gruppentheoretische Studien », *Math. Ann.*, vol. 20, n<sup>o</sup> 1, 1882, p. 1-44 (lire en ligne<sup>[[archive](#)]</sup>).

17. † Camille Jordan, « Commentaires sur Galois », *Math. Ann.*, vol. 1, n° 2, 1869, p. 141-160 ([lire en ligne](#) [\[archive\]](#)).
18. † Camille Jordan, *Traité des substitutions et des équations algébriques*, Gauthier-Villars, 1870 ([lire en ligne](#) [\[archive\]](#)), p. 389-395.
19. † **(en)** B. L. van der Waerden, *A History of Algebra*, Springer, 1980 (ISBN 038713610X), p. 124.
20. † **(de)** Heinrich Weber, « Die allgemeinen Grundlagen der Galois'schen Gleichungstheorie », *Math. Ann.*, vol. 43, 1893, p. 521-549 ([lire en ligne](#) [\[archive\]](#)).
21. † **(de)** Ernst Kummer, « Über die Zerlegung der aus Wurzeln der Einheit gebildeten complexen Zahlen in ihre Primfactoren », *J. reine angew. Math.*, vol. 35, 1847, p. 327-367 [[lire en ligne](#) [\[archive\]](#)].
22. † Richard Dedekind, *Sur la théorie des nombres entiers algébriques*, 1871.
23. † **(de)** Felix Klein, *Vorlesungen über das Ikosaeder und die Auflösung der Gleichungen fünften Grades*, Teubner, Leipzig, 1884.
24. † **(de)** David Hilbert, « Über die Theorie des relativ-quadratischen Zahlkörpers », *Math. Ann.*, vol. 51, 1899, p. 1-127.
25. † **(en)** Emil Artin et Arthur Milgram, *Galois Theory*, Dover, 1998 (ISBN 9780486623429) (1<sup>re</sup> éd. 1942) [[lire en ligne](#) [\[archive\]](#)].
26. † Henri Cartan, « Théorie de Galois pour les corps non commutatifs », *ASENS*, 3<sup>e</sup> série, t. 64, n° 7, 1947, p. 59-77 ([lire en ligne](#) [\[archive\]](#)).
27. † **(en)** Nathan Jacobson, *Structure of Rings*, Amer. Math. Soc., Providence, 1956 p. 163 [\[archive\]](#).
28. † Jean Dieudonné, « Généralisation de la théorie de Galois », *Séminaire Dubreil. Algèbre et théorie des nombres*, t. 1, 1947-1948, p. 1-6 ([lire en ligne](#) [\[archive\]](#)).
29. † Une présentation unifiée de ces travaux peut être trouvée dans **(en)** Paul M. Cohn, *Skew fields - Theory of general division rings*, Cambridge University Press, 1995 ([lire en ligne](#) [\[archive\]](#)).
30. † **(en)** Stephen Urban Chase et Moss E. Sweedler **(en)**, *Hopf Algebra and Galois Theory*, Springer, 1969 ([lire en ligne](#) [\[archive\]](#)).

Voir aussi [ [modifier](#) | [modifier le code](#) ]

## Bibliographie [ [modifier](#) | [modifier le code](#) ]

- **(en)** Jörg Bewersdorff (trad. de l'allemand), *Galois Theory for Beginners: A Historical Perspective* [« Algebra für Einsteiger: Von der Gleichungsauflösung zur Galois-Theorie »], AMS, 2006 ([lire en ligne](#) [\[archive\]](#))
- Jean-Claude Carrega, *Théorie des corps - La règle et le compas* [[détail de l'édition](#)]
- **(en)** David A. Cox, *Galois Theory*, John Wiley & Sons, 2012, 2<sup>e</sup> éd. (1<sup>re</sup> éd. 2004) ([lire en ligne](#) [\[archive\]](#))
- Régine et Adrien Douady, *Algèbre et théories galoisiennes* [[détail des éditions](#)]
- É. Galois, *Écrits et Mémoires Mathématiques d'Évariste Galois*, Gauthier-Villars, Paris, 1962
- É. Galois et G. Verriest, *Œuvres Mathématiques d'Évariste Galois, publiées en 1897, suivies d'une notice sur Évariste Galois et la théorie des équations algébriques*, Gauthier-Villars, Paris, 1951
- Ivan Gozard, *Théorie de Galois*, 2<sup>e</sup> éd., Paris, Ellipses, 2009
- **(en)** Charles Robert Hadlock, *Field Theory and Its Classical Problems*, MAA, coll. « The Carus Mathematical Monographs » (n° 19), 2000 ([lire en ligne](#) [\[archive\]](#)) — agréable à lire, les prérequis sont très modestes
- David Hernandez et Yves Laszlo, *Introduction à la théorie de Galois*, Éditions de l'École polytechnique, 2012 [[présentation en ligne](#) [\[archive\]](#)]
- Serge Lang, *Algèbre* [[détail des éditions](#)]
- **(en)** Joseph Rotman **(en)**, *Galois Theory*, Springer, 1998, 2<sup>e</sup> éd. (1<sup>re</sup> éd. 1990) ([lire en ligne](#) [\[archive\]](#))

- Pierre Samuel, *Théorie algébrique des nombres* [détail de l'édition]
- (en) Ian Stewart, *Galois Theory*, CRC Press, 2015, 4<sup>e</sup> éd. (lire en ligne  [archive]) — idem Hadlock 2000
- (en) Jean-Pierre Tignol, *Galois' Theory of Algebraic Equations*, World Scientific, 2015, 2<sup>e</sup> éd. (1<sup>re</sup> éd. 2001) (lire en ligne  [archive])

## Liens externes

[modifier | modifier le code]

- Bernard Bychan, Les archives de Évariste Galois  [archive]
- Alain Kraus, Un cours de DEA sur la théorie de Galois  [archive] **[PDF]** (université Paris 6, 1998)
- Colas Bardavid, Un cours niveau premier cycle de théorie de Galois élémentaire  [archive] **[PDF]**
- (en) Résumé de la théorie de Galois  [archive] extraits de John A. Beachy et William D. Blair, *Abstract Algebra*, 2<sup>e</sup> éd.

v · m	<b>Théorie de Galois</b> <span>[masquer]</span>
<b>Corps</b>	Corps fini · Corps parfait · Corps de rupture · Corps de décomposition
<b>Extension de corps</b>	Extension algébrique · Extension quadratique · Extension simple · Extension normale · Extension séparable · Extension de Galois · Groupe de Galois · Clôture algébrique · Extension radicielle · Corps de fonctions
<b>Articles associés</b>	Caractéristique · Polynôme formel · Polynôme cyclotomique · <b>Théorie de Galois</b> · Théorème fondamental de la théorie de Galois · Théorème de l'élément primitif · Extension des morphismes et des places dans les anneaux intègres et les corps · Théorie d'Iwasawa



**Portail des mathématiques**

Catégories : Théorie de Galois | Évariste Galois [+]

La dernière modification de cette page a été faite le 8 janvier 2019 à 10:11.

**Droit d'auteur** : les textes sont disponibles sous licence Creative Commons attribution, partage dans les mêmes conditions ; d'autres conditions peuvent s'appliquer. Voyez les conditions d'utilisation pour plus de détails, ainsi que les crédits graphiques. En cas de réutilisation des textes de cette page, voyez comment citer les auteurs et mentionner la licence. Wikipedia® est une marque déposée de la Wikimedia Foundation, Inc., organisation de bienfaisance régie par le paragraphe 501(c)(3) du code fiscal des États-Unis.

Politique de confidentialité À propos de Wikipédia Avertissements Contact Développeurs

Déclaration sur les témoins (cookies) Version mobile

