La « théorie de Galois » et son enseignement

Antoine Chambert-Loir

Institut de recherche mathématique de Rennes, Université de Rennes 1

Bicentenaire de la naissance d'Évariste Galois
24 octobre 2011

Qu’est-ce que la théorie de Galois ?

Gilles **Châtelet** :
« La physique mathématique comme projet »
L’enchantement du virtuel. Mathématique, physique, philosophie
édité par C. Alluni et C. Paoletti, ÉditionsRued’Ulm, 2010.

« La théorie des équations de Galois constitue probablement un des plus beaux exemples du principe de dissymétrie créatrice en mathématiques. Cette théorie des équations (...) prend explicitement pour thème la symétrie et la dissymétrie de l’ensemble des racines d’une équation irréductible à coefficients entiers,

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0 \qquad \text{(E)}$$

Qu’est-ce que la théorie de Galois ?

Gilles **Châtelet** :
« La physique mathématique comme projet »
L’enchantement du virtuel. Mathématique, physique, philosophie
édité par C. Alluni et C. Paoletti, ÉditionsRued’Ulm, 2010.

« Rappelons que les travaux de Cauchy avaient déjà montré l’existence d’un domaine $D(\alpha_1, \ldots, \alpha_n)$ étendant les rationnels et sur lequel (E) se décompose :

$$(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n) = 0$$

« L’indexation des racines sous la forme (α_i) est tout à fait arbitraire. Pour l’algébriste qui calcule sur les rationnels, ces racines n’existent pas. Ce qui existe c’est le domaine $D(\alpha_1, \ldots, \alpha_n)$ et la manière dont il s’obtient à partir de (E).

Qu’est-ce que la théorie de Galois ?

Gilles **Châtelet** :
« La physique mathématique comme projet »
L’enchantement du virtuel. Mathématique, physique, philosophie
édité par C. Alluni et C. Paoletti, ÉditionsRued’Ulm, 2010.

« À proprement parler, ces racines ne sont pas « possibles ». Elles créent « du possible » au sens où le domaine $D(\alpha_1, \ldots, \alpha_n)$ est d’autant plus vaste que les substitutions que peut effectuer un algébriste ne connaissant que les rationnels sont plus nombreuses. Ces substitutions peuvent être toutes les permutations qui échangent les racines. Il peut exister aussi des relations rationnelles « particulières » entre elles (équations « bicarrées », équations « réciproques »).

Qu’est-ce que la théorie de Galois ?

Gilles **Châtelet** :
« La physique mathématique comme projet »
L’enchantement du virtuel. Mathématique, physique, philosophie
édité par C. Alluni et C. Paoletti, ÉditionsRued’Ulm, 2010.

« Le groupe de symétrie de l’équation (groupe de Galois) est alors le plus grand groupe de substitutions qui respecte les relations entre les racines. Il traduit notre manque de discernement entre les (α_i) mais apprécie également la dimension du nouveau domaine de rationalité $D(\alpha_1, \ldots, \alpha_n)$ qu’il constitue. Il mesure bien l’espace de liberté engendré par le problème. Ces racines n’existent que virtuellement. Elles n’agissent pas comme individus mais par la potentialité de leurs échanges. »

Corps commutatifs

La « théorie de Galois » vise à expliquer, classifier, décrire les **corps** et leurs **extensions**.

Corps : ensemble F muni d'une addition $+$, d'une multiplication $\times$, commutatives et associatives, la multiplication étant distributive par rapport à la multiplication. On suppose l'existence d'un élément neutre 0 pour l'addition, d'un élément neutre 1 pour la multiplication (et $1 \neq 0$), que tout élément a un opposé (pour $+$) et que tout élément non nul a un inverse (pour $\times$).

Corps commutatifs

La « théorie de Galois » vise à expliquer, classifier, décrire les **corps** et leurs **extensions**.

Corps : ensemble F muni d'une addition $+$, d'une multiplication $\times$, commutatives et associatives, la multiplication étant distributive par rapport à la multiplication. On suppose l'existence d'un élément neutre 0 pour l'addition, d'un élément neutre 1 pour la multiplication (et $1 \neq 0$), que tout élément a un opposé (pour $+$) et que tout élément non nul a un inverse (pour $\times$).

Corps commutatifs : exemples

Exemples : 1) le corps **Q** des nombres rationnels ;
2) ceux **R** et **C** des nombres réels ou des nombres complexes ;
3) les corps de restes $\mathbf{Z}/p\mathbf{Z}$ (p nombre premier), les corps finis $\mathbf{F}_q$ (q puissance d'un nombre premier) ;
4) le corps des fonctions méromorphes sur une surface de Riemann connexe, celui des fonctions rationnelles sur une variété algébrique irréductible...

Extensions de corps

Extension de corps : application $F \hookrightarrow F'$ où F et F' sont deux corps, envoyant 0 sur 0, 1 sur 1 et compatible à l'addition et à la multiplication.

Exemples : 1) si P est un polynôme à coefficients entiers, l'inclusion de $\mathbf{Q}$ dans le sous-corps $\mathbf{Q}(\alpha_1, \ldots, \alpha_n)$ de $\mathbf{C}$ engendré par les racines $\alpha_1, \ldots, \alpha_n$ de P ;

2) si q est une puissance d'un nombre premier p, l'inclusion de corps finis $\mathbf{F}_p \hookrightarrow \mathbf{F}_q$;

3) si $f : M' \to M$ est un morphisme non constant de surfaces de Riemann connexes compactes, l'extension $f^* : \mathbf{C}(M) \hookrightarrow \mathbf{C}(M')$ obtenue par composition par f des fonctions méromorphes sur M ;

4) l'extension analogue si $f : M' \to M$ est un morphisme dominant de variétés algébriques irréductibles.

Extensions de corps

Extension de corps : application $F \hookrightarrow F'$ où F et F' sont deux corps, envoyant 0 sur 0, 1 sur 1 et compatible à l'addition et à la multiplication.

Exemples : 1) si P est un polynôme à coefficients entiers, l'inclusion de $\mathbf{Q}$ dans le sous-corps $\mathbf{Q}(\alpha_1, \ldots, \alpha_n)$ de $\mathbf{C}$ engendré par les racines $\alpha_1, \ldots, \alpha_n$ de P ;

2) si q est une puissance d'un nombre premier p, l'inclusion de corps finis $\mathbf{F}_p \hookrightarrow \mathbf{F}_q$;

3) si $f : M' \to M$ est un morphisme non constant de surfaces de Riemann connexes compactes, l'extension $f^* : \mathbf{C}(M) \hookrightarrow \mathbf{C}(M')$ obtenue par composition par f des fonctions méromorphes sur M ;

4) l'extension analogue si $f : M' \to M$ est un morphisme dominant de variétés algébriques irréductibles.

Extensions de corps

Extension de corps : application $F \hookrightarrow F'$ où F et F' sont deux corps, envoyant 0 sur 0, 1 sur 1 et compatible à l'addition et à la multiplication.

Exemples : 1) si P est un polynôme à coefficients entiers, l'inclusion de $\mathbf{Q}$ dans le sous-corps $\mathbf{Q}(\alpha_1, \ldots, \alpha_n)$ de $\mathbf{C}$ engendré par les racines $\alpha_1, \ldots, \alpha_n$ de P ;

2) si q est une puissance d'un nombre premier p, l'inclusion de corps finis $\mathbf{F}_p \hookrightarrow \mathbf{F}_q$;

3) si $f : M' \to M$ est un morphisme non constant de surfaces de Riemann connexes compactes, l'extension $f^* : \mathbf{C}(M) \hookrightarrow \mathbf{C}(M')$ obtenue par composition par f des fonctions méromorphes sur M ;

4) l'extension analogue si $f : M' \to M$ est un morphisme dominant de variétés algébriques irréductibles.

Extensions de corps

Extension de corps : application $F \hookrightarrow F'$ où F et F' sont deux corps, envoyant 0 sur 0, 1 sur 1 et compatible à l'addition et à la multiplication.

Exemples : 1) si P est un polynôme à coefficients entiers, l'inclusion de $\mathbf{Q}$ dans le sous-corps $\mathbf{Q}(\alpha_1, \ldots, \alpha_n)$ de $\mathbf{C}$ engendré par les racines $\alpha_1, \ldots, \alpha_n$ de P ;

2) si q est une puissance d'un nombre premier p, l'inclusion de corps finis $\mathbf{F}_p \hookrightarrow \mathbf{F}_q$;

3) si $f : M' \to M$ est un morphisme non constant de surfaces de Riemann connexes compactes, l'extension $f^* : \mathbf{C}(M) \hookrightarrow \mathbf{C}(M')$ obtenue par composition par f des fonctions méromorphes sur M ;

4) l'extension analogue si $f : M' \to M$ est un morphisme dominant de variétés algébriques irréductibles.

Éléments algébriques

Considérons une extension de corps $F \hookrightarrow F'$.

Un élément α de F' est **algébrique** sur F s'il est solution dans F' d'une équation polynomiale (non idiote) à coefficients dans F.
Il est alors racine d'un unique polynôme unitaire de degré minimal, irréductible, qu'on appelle son **polynôme minimal**.
Son degré est aussi appelé **degré de** α.

Exemples : 1) $\sqrt{2}$ est de degré 2 sur $\mathbf{Q}$, son polynôme minimal est $X^2 - 2$.

2) $\exp(2i\pi/17)$ est racine du polynôme

$$(X^{17} - 1)/(X - 1) = X^{16} + X^{15} + \cdots + 1$$

Comme ce polynôme est irréductible, il est de degré 16.

3) e, π ne sont pas algébriques sur $\mathbf{Q}$.

Éléments algébriques

Considérons une extension de corps $F \hookrightarrow F'$.

Un élément α de F' est **algébrique** sur F s'il est solution dans F' d'une équation polynomiale (non idiote) à coefficients dans F.
Il est alors racine d'un unique polynôme unitaire de degré minimal, irréductible, qu'on appelle son **polynôme minimal**.
Son degré est aussi appelé **degré de** α.

Exemples : 1) $\sqrt{2}$ est de degré 2 sur $\mathbf{Q}$, son polynôme minimal est $X^2 - 2$.

2) $\exp(2i\pi/17)$ est racine du polynôme

$$(X^{17} - 1)/(X - 1) = X^{16} + X^{15} + \cdots + 1$$

Comme ce polynôme est irréductible, il est de degré 16.

3) e, π ne sont pas algébriques sur $\mathbf{Q}$.

Extensions algébriques

Une extension $F \hookrightarrow F'$ est dite algébrique si tout élément de F' est algébrique sur F.

Exemples : 1) extensions $F \hookrightarrow F'$ telles que F' est engendré par des éléments algébriques sur F ;
concrètement : $\mathbf{Q} \hookrightarrow \mathbf{Q}(\sqrt[3]{2})$, $\mathbf{Q} \hookrightarrow \mathbf{Q}(\sqrt[3]{2}, \exp(2\mathrm{i}\pi/3))$,...

2) **extensions finies**, c'est-à-dire telles que F' soit un F-espace vectoriel de dimension finie — on note alors $[F' : F] = \dim_F(F')$ le degré de l'extension.

Extensions algébriques

Une extension $F \hookrightarrow F'$ est dite algébrique si tout élément de F' est algébrique sur F.

Exemples : 1) extensions $F \hookrightarrow F'$ telles que F' est engendré par des éléments algébriques sur F ;
concrètement : $\mathbf{Q} \hookrightarrow \mathbf{Q}(\sqrt[3]{2})$, $\mathbf{Q} \hookrightarrow \mathbf{Q}(\sqrt[3]{2}, \exp(2\mathrm{i}\pi/3))$,...

2) **extensions finies**, c'est-à-dire telles que F' soit un F-espace vectoriel de dimension finie — on note alors $[F' : F] = \dim_F(F')$ le degré de l'extension.

Extensions algébriques

Une extension $F \hookrightarrow F'$ est dite algébrique si tout élément de F' est algébrique sur F.

Exemples : 1) extensions $F \hookrightarrow F'$ telles que F' est engendré par des éléments algébriques sur F ;
concrètement : $\mathbf{Q} \hookrightarrow \mathbf{Q}(\sqrt[3]{2})$, $\mathbf{Q} \hookrightarrow \mathbf{Q}(\sqrt[3]{2}, \exp(2\mathrm{i}\pi/3))$,...

2) **extensions finies**, c'est-à-dire telles que F' soit un F-espace vectoriel de dimension finie — on note alors $[F' : F] = \dim_F(F')$ le degré de l'extension.

Construction d'extensions algébriques

Soit F un corps et soit P un polynôme à coefficients dans F.
On peut construire une **extension de décomposition**, une extension algébrique $F \hookrightarrow F_P$ telle que :

1) le polynôme P est scindé dans F_P ;

2) le corps F_P est engendré sur F par les racines de P dans F_P.

Une telle extension est « unique »,
au sens où toute extension $F \hookrightarrow F'_P$ vérifiant ces propriétés est *isomorphe* à l'extension donnée $F \hookrightarrow F_P$.

La « théorie de Galois » semble être une espèce de version statique de la théorie de Galois dans laquelle les racines ne vivent que pour être permutées.
C'est la *multiplicité des isomorphismes* entre les extensions F_P et F'_P qui restaure, au sein de la « théorie de Galois » la dynamique inhérente à la théorie de Galois.

Construction d’extensions algébriques

Soit F un corps et soit P un polynôme à coefficients dans F.
On peut construire une **extension de décomposition**,
une extension algébrique $F \hookrightarrow F_P$ telle que :

1) le polynôme P est scindé dans F_P ;
2) le corps F_P est engendré sur F par les racines de P dans F_P.

Une telle extension est « unique »,
au sens où toute extension $F \hookrightarrow F'_P$ vérifiant ces propriétés est *isomorphe* à l’extension donnée $F \hookrightarrow F_P$.

La « théorie de Galois » semble être une espèce de version statique de la théorie de Galois dans laquelle les racines ne vivent que pour être permutées.
C’est la *multiplicité des isomorphismes* entre les extensions F_P et F'_P qui restaure, au sein de la « théorie de Galois » la dynamique inhérente à la théorie de Galois.

Construction d’extensions algébriques

Soit F un corps et soit P un polynôme à coefficients dans F.
On peut construire une **extension de décomposition**,
une extension algébrique $F \hookrightarrow F_P$ telle que :

1) le polynôme P est scindé dans F_P ;
2) le corps F_P est engendré sur F par les racines de P dans F_P.

Une telle extension est « unique »,
au sens où toute extension $F \hookrightarrow F'_P$ vérifiant ces propriétés est *isomorphe* à l’extension donnée $F \hookrightarrow F_P$.

La « théorie de Galois » semble être une espèce de version statique de la théorie de Galois dans laquelle les racines ne vivent que pour être permutées.
C’est la *multiplicité des isomorphismes* entre les extensions F_P et F'_P qui restaure, au sein de la « théorie de Galois » la dynamique inhérente à la théorie de Galois.

Le groupe de Galois d'une extension algébrique

Considérons une extension de corps $F \hookrightarrow F'$, algébrique.

Son **groupe de Galois**, noté $\mathrm{Gal}(F'/F)$, est l'ensemble des automorphismes de corps de F' qui fixent tout élément de F.

Autrement dit, un élement de $\mathrm{Gal}(F'/F)$ est une bijection de F' qui fixe tout élément de F et qui est compatible avec l'addition et la multiplication.

La composition des bijections fait de $\mathrm{Gal}(F'/F)$ un **groupe**.

Exemples : 1) le corps $\mathbf{C}$ a exactement deux automorphismes qui fixent $\mathbf{R}$, l'identité et la conjugaison complexe c. Ainsi, $\mathrm{Gal}(\mathbf{C}/\mathbf{R}) = \{\mathrm{Id}, c\}$ est le groupe à deux éléments ;

2) le corps $\mathbf{Q}(\sqrt[3]{2})$ n'a aucun automorphisme autre que l'identité, et $\mathrm{Gal}(\mathbf{Q}(\sqrt[3]{2})/\mathbf{Q}) = \{\mathrm{Id}\}$.

Le groupe de Galois d'une extension algébrique

Considérons une extension de corps $F \hookrightarrow F'$, algébrique.

Son **groupe de Galois**, noté $\mathrm{Gal}(F'/F)$, est l'ensemble des automorphismes de corps de F' qui fixent tout élément de F.

Autrement dit, un élement de $\mathrm{Gal}(F'/F)$ est une bijection de F' qui fixe tout élément de F et qui est compatible avec l'addition et la multiplication.

La composition des bijections fait de $\mathrm{Gal}(F'/F)$ un **groupe**.

Exemples : 1) le corps $\mathbf{C}$ a exactement deux automorphismes qui fixent $\mathbf{R}$, l'identité et la conjugaison complexe c. Ainsi, $\mathrm{Gal}(\mathbf{C}/\mathbf{R}) = \{\mathrm{Id}, c\}$ est le groupe à deux éléments ;

2) le corps $\mathbf{Q}(\sqrt[3]{2})$ n'a aucun automorphisme autre que l'identité, et $\mathrm{Gal}(\mathbf{Q}(\sqrt[3]{2})/\mathbf{Q}) = \{\mathrm{Id}\}$.

Le groupe de Galois d'une extension algébrique

Considérons une extension de corps $F \hookrightarrow F'$, algébrique.

Son **groupe de Galois**, noté $\mathrm{Gal}(F'/F)$, est l'ensemble des automorphismes de corps de F' qui fixent tout élément de F.

Autrement dit, un élement de $\mathrm{Gal}(F'/F)$ est une bijection de F' qui fixe tout élément de F et qui est compatible avec l'addition et la multiplication.

La composition des bijections fait de $\mathrm{Gal}(F'/F)$ un **groupe**.

Exemples : 1) le corps $\mathbf{C}$ a exactement deux automorphismes qui fixent $\mathbf{R}$, l'identité et la conjugaison complexe c. Ainsi, $\mathrm{Gal}(\mathbf{C}/\mathbf{R}) = \{\mathrm{Id}, c\}$ est le groupe à deux éléments ;

2) le corps $\mathbf{Q}(\sqrt[3]{2})$ n'a aucun automorphisme autre que l'identité, et $\mathrm{Gal}(\mathbf{Q}(\sqrt[3]{2})/\mathbf{Q}) = \{\mathrm{Id}\}$.

Le groupe de Galois d'une extension algébrique

Considérons une extension de corps $F \hookrightarrow F'$, algébrique.

Son **groupe de Galois**, noté $\mathrm{Gal}(F'/F)$, est l'ensemble des automorphismes de corps de F' qui fixent tout élément de F.

Autrement dit, un élement de $\mathrm{Gal}(F'/F)$ est une bijection de F' qui fixe tout élément de F et qui est compatible avec l'addition et la multiplication.

La composition des bijections fait de $\mathrm{Gal}(F'/F)$ un **groupe**.

Exemples : 1) le corps $\mathbf{C}$ a exactement deux automorphismes qui fixent $\mathbf{R}$, l'identité et la conjugaison complexe c. Ainsi, $\mathrm{Gal}(\mathbf{C}/\mathbf{R}) = \{\mathrm{Id}, c\}$ est le groupe à deux éléments ;

2) le corps $\mathbf{Q}(\sqrt[3]{2})$ n'a aucun automorphisme autre que l'identité, et $\mathrm{Gal}(\mathbf{Q}(\sqrt[3]{2})/\mathbf{Q}) = \{\mathrm{Id}\}$.

Extensions galoisiennes

Ce sont celles qui possèdent toute la dynamique de la « théorie de Galois ».

On dit qu'une extension (algébrique, finie) $F \hookrightarrow F'$ est **galoisienne** si elle vérifie l'une des propriétés équivalentes suivantes :

1) pour tout élément $\alpha \in F' \setminus F$, il existe $g \in \mathrm{Gal}(F'/F)$ tel que $g(\alpha) \neq \alpha$;

2) le degré $[F' : F]$ de l'extension est égal au cardinal du groupe $\mathrm{Gal}(F'/F)$;

3) le polynôme minimal de tout élément de F' est scindé à racines simples dans F' ;

4) le corps F' est engendré sur F par les racines d'un polynôme $P \in F[X]$ qui est *scindé à racines simples* dans F'.

Extensions galoisiennes

Ce sont celles qui possèdent toute la dynamique de la « théorie de Galois ».

On dit qu'une extension (algébrique, finie) $F \hookrightarrow F'$ est **galoisienne** si elle vérifie l'une des propriétés équivalentes suivantes :

1) pour tout élément $\alpha \in F' \setminus F$, il existe $g \in \mathrm{Gal}(F'/F)$ tel que $g(\alpha) \neq \alpha$;

2) le degré $[F' : F]$ de l'extension est égal au cardinal du groupe $\mathrm{Gal}(F'/F)$;

3) le polynôme minimal de tout élément de F' est scindé à racines simples dans F' ;

4) le corps F' est engendré sur F par les racines d'un polynôme $P \in F[X]$ qui est *scindé à racines simples* dans F'.

Extensions galoisiennes (commentaire)

Des quatre conditions équivalentes précédentes, les deux premières sont deux façons de mesurer le « dynamisme » de l'extension $F \hookrightarrow F'$: la première dit que le groupe $\mathrm{Gal}(F'/F)$ *bouge assez* F', la seconde qu'il est aussi *gros* que possible.

La troisième explique la seule cause possible de l'asthénie d'une extension $F \hookrightarrow F'$: l'absence dans F' d'assez de *conjugués* des éléments de F'.

La quatrième fournit un moyen concret de construire une extension galoisienne : c'est une extension de décomposition $F \hookrightarrow F_P$ d'un polynôme P dont toutes les racines seront simples. Cette dernière condition, de **séparabilité**, est automatique en caractéristique zéro ou sur les corps finis, mais son développement est un peu délicat.

Extensions galoisiennes (commentaire)

Des quatre conditions équivalentes précédentes, les deux premières sont deux façons de mesurer le « dynamisme » de l'extension $F \hookrightarrow F'$: la première dit que le groupe $\mathrm{Gal}(F'/F)$ *bouge assez* F', la seconde qu'il est aussi *gros* que possible.

La troisième explique la seule cause possible de l'asthénie d'une extension $F \hookrightarrow F'$: l'absence dans F' d'assez de *conjugués* des éléments de F'.

La quatrième fournit un moyen concret de construire une extension galoisienne : c'est une extension de décomposition $F \hookrightarrow F_P$ d'un polynôme P dont toutes les racines seront simples. Cette dernière condition, de **séparabilité**, est automatique en caractéristique zéro ou sur les corps finis, mais son développement est un peu délicat.

Extensions galoisiennes (commentaire)

Des quatre conditions équivalentes précédentes, les deux premières sont deux façons de mesurer le « dynamisme » de l'extension $F \hookrightarrow F'$: la première dit que le groupe $\mathrm{Gal}(F'/F)$ *bouge assez* F', la seconde qu'il est aussi *gros* que possible.

La troisième explique la seule cause possible de l'asthénie d'une extension $F \hookrightarrow F'$: l'absence dans F' d'assez de *conjugués* des éléments de F'.

La quatrième fournit un moyen concret de construire une extension galoisienne : c'est une extension de décomposition $F \hookrightarrow F_P$ d'un polynôme P dont toutes les racines seront simples. Cette dernière condition, de **séparabilité**, est automatique en caractéristique zéro ou sur les corps finis, mais son développement est un peu délicat.

La « théorie de Galois »

Il s'agit d'une correspondance, d'un dictionnaire, entre **sous-extensions** d'une extension galoisienne et **sous-groupes** de son groupe de Galois.

Soit $F \hookrightarrow F'$ une extension galoisienne, soit $G = \mathrm{Gal}(F'/F)$.
À tout sous-groupe H de G, on associe le corps $(F')^H$ formé des éléments de F' fixés par tout élément de H ; il contient F.
À tout sous-corps E de F' contenant F, on associe le sous-groupe $\mathrm{Gal}(F'/E)$ de G.

Ces opérations $H \rightsquigarrow (F')^H$ et $E \rightsquigarrow \mathrm{Gal}(F'/E)$ sont des bijections réciproques l'une de l'autre.
De plus, l'extension E/F est galoisienne si et seulement si le sous-groupe H est distingué dans G.

La « théorie de Galois »

Il s'agit d'une correspondance, d'un dictionnaire, entre **sous-extensions** d'une extension galoisienne et **sous-groupes** de son groupe de Galois.

Soit $F \hookrightarrow F'$ une extension galoisienne, soit $G = \mathrm{Gal}(F'/F)$.
À tout sous-groupe H de G, on associe le corps $(F')^H$ formé des éléments de F' fixés par tout élément de H ; il contient F.
À tout sous-corps E de F' contenant F, on associe le sous-groupe $\mathrm{Gal}(F'/E)$ de G.

Ces opérations $H \rightsquigarrow (F')^H$ et $E \rightsquigarrow \mathrm{Gal}(F'/E)$ sont des bijections réciproques l'une de l'autre.
De plus, l'extension E/F est galoisienne si et seulement si le sous-groupe H est distingué dans G.

La « théorie de Galois »

Il s'agit d'une correspondance, d'un dictionnaire, entre **sous-extensions** d'une extension galoisienne et **sous-groupes** de son groupe de Galois.

Soit $F \hookrightarrow F'$ une extension galoisienne, soit $G = \mathrm{Gal}(F'/F)$.
À tout sous-groupe H de G, on associe le corps $(F')^H$ formé des éléments de F' fixés par tout élément de H ; il contient F.
À tout sous-corps E de F' contenant F, on associe le sous-groupe $\mathrm{Gal}(F'/E)$ de G.

Ces opérations $H \rightsquigarrow (F')^H$ et $E \rightsquigarrow \mathrm{Gal}(F'/E)$ sont des bijections réciproques l'une de l'autre.
De plus, l'extension E/F est galoisienne si et seulement si le sous-groupe H est distingué dans G.

Exemples de groupes de Galois

Le calcul du groupe de Galois est un problème ardu. Considérons un polynôme séparable $P \in F[X]$, une extension de décomposition $F \hookrightarrow F_P$ et son groupe de Galois $G = \mathrm{Gal}(F_P/F)$.

Exemples de groupes de Galois

Le calcul du groupe de Galois est un problème ardu. Considérons un polynôme séparable $P \in F[X]$, une extension de décomposition $F \hookrightarrow F_P$ et son groupe de Galois $G = \mathrm{Gal}(F_P/F)$.

1) Le groupe G est naturellement un sous-groupe du groupe des permutations des racines de P dans F_P. C'est un sous-groupe **transitif** si et seulement si P est irréductible.

Exemples de groupes de Galois

Le calcul du groupe de Galois est un problème ardu. Considérons un polynôme séparable $P \in F[X]$, une extension de décomposition $F \hookrightarrow F_P$ et son groupe de Galois $G = \mathrm{Gal}(F_P/F)$.

1) Le groupe G est naturellement un sous-groupe du groupe des permutations des racines de P dans F_P. C'est un sous-groupe **transitif** si et seulement si P est irréductible.

2) En degré 3, on trouve $G = \mathfrak{A}_3$ si le discriminant de P est un carré, $\mathfrak{S}_3$ sinon.
NB. Le discriminant de $P = X^3 + pX + q$ est $-4p^3 - 27q^2$.

Exemples de groupes de Galois

Le calcul du groupe de Galois est un problème ardu. Considérons un polynôme séparable $P \in F[X]$, une extension de décomposition $F \hookrightarrow F_P$ et son groupe de Galois $G = \mathrm{Gal}(F_P/F)$.

1) Le groupe G est naturellement un sous-groupe du groupe des permutations des racines de P dans F_P. C'est un sous-groupe **transitif** si et seulement si P est irréductible.

2) En degré 3, on trouve $G = \mathfrak{A}_3$ si le discriminant de P est un carré, $\mathfrak{S}_3$ sinon.
NB. Le discriminant de $P = X^3 + pX + q$ est $-4p^3 - 27q^2$.

3) Si $F = k(a_1, \ldots, a_n)$ et $P = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ est l'équation générale, on a $G = \mathfrak{S}_n$.

Exemples de groupes de Galois

Le calcul du groupe de Galois est un problème ardu. Considérons un polynôme séparable $P \in F[X]$, une extension de décomposition $F \hookrightarrow F_P$ et son groupe de Galois $G = \mathrm{Gal}(F_P/F)$.

4) Si $P = X^n - 1$ et $F = \mathbf{Q}$, on a $G = (\mathbf{Z}/n\mathbf{Z})^*$ — irréductibilité du polynôme cyclotomique.

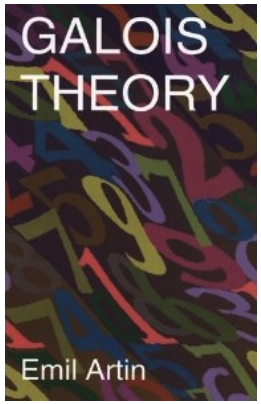
Exemples de groupes de Galois

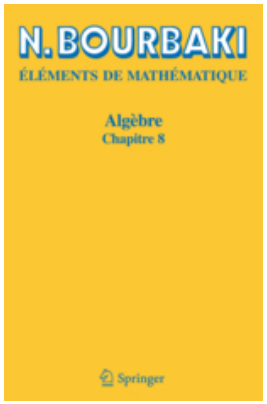
Le calcul du groupe de Galois est un problème ardu. Considérons un polynôme séparable $P \in F[X]$, une extension de décomposition $F \hookrightarrow F_P$ et son groupe de Galois $G = \mathrm{Gal}(F_P/F)$.

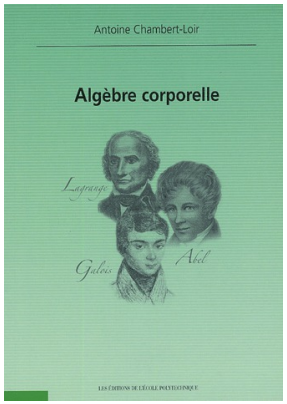
4) Si $P = X^n - 1$ et $F = \mathbf{Q}$, on a $G = (\mathbf{Z}/n\mathbf{Z})^*$ — irréductibilité du polynôme cyclotomique.

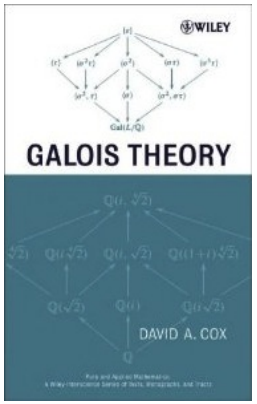
5) Si $P = X^n - 2$ et $F = \mathbf{Q}$, la suite d'extensions $\mathbf{Q} \hookrightarrow F_{X^n-1} \hookrightarrow F_{X^n-2}$ fournit un sous-groupe distingué $H \subset G$ isomorphe à $\mathbf{Z}/n\mathbf{Z}$ et G/H est isomorphe à $(\mathbf{Z}/n\mathbf{Z})^*$.

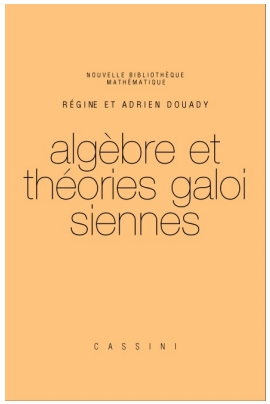
Apprendre la « théorie de Galois » ?

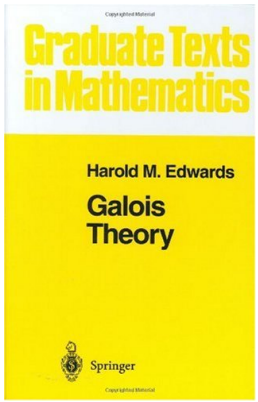


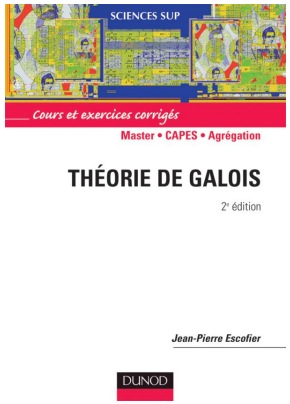


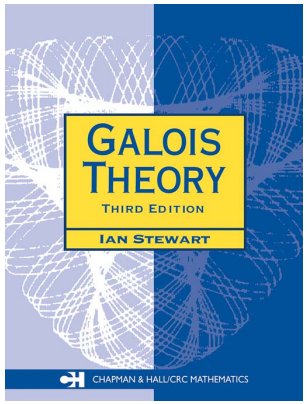


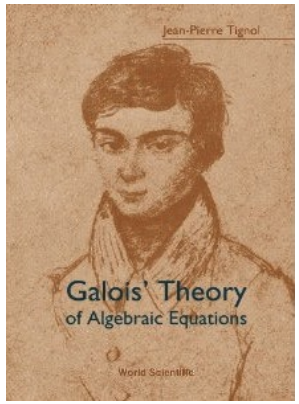


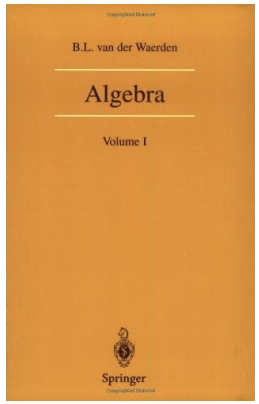












Approches de la « théorie de Galois »

1) *Utilisation d'un élément primitif*

Si $F \hookrightarrow F'$ est une extension finie séparable, on démontre qu'il existe un **élément primitif** $\alpha \in F'$ tel que $F' = F[\alpha]$. Alors, les automorphismes de F' correspondent aux conjugués de α dans F'. Si le polynôme minimal P de α est scindé dans F', on voit donc que
$\mathrm{Card}(\mathrm{Gal}(F'/F)) = \deg(P) = [F' : F]$.
Si $F_1 = (F')^{\mathrm{Gal}(F'/F)}$, on a encore $\mathrm{Gal}(F'/F_1) = \mathrm{Gal}(F'/F)$, et comme ce qui précède s'applique aussi à l'extension $F_1 \hookrightarrow F'$, on a $[F' : F] = [F' : F_1]$, d'où $F = F_1$.

Approches de la « théorie de Galois »

1) *Utilisation d'un élément primitif*

2) *Lemme d'Artin*

On évite le recours à un élément primitif par un dévissage. Il faut prouver directement le **lemme d'Artin :** si G est un groupe fini d'automorphismes d'un corps F' et si $F = (F')^G$, alors l'extension $F \hookrightarrow F'$ est finie de degré Cαrd(G).

Approches de la « théorie de Galois »

1) *Utilisation d'un élément primitif*

2) *Lemme d'Artin*

3) *Lemme de Dedekind et descente galoisienne*

Cette approche tire profit de ce que « la théorie de Galois est trivialisée par descente galoisienne ». C'est celle de Bourbaki (2$^{\text{de}}$ édition) qui introduit au passage la notion d'**algèbre étale** :
une extension finie $F \hookrightarrow F'$ est galoisienne si et seulement si le produit tensoriel $F' \otimes_F F'$ est isomorphe à une algèbre $(F')^n$, où $n = [F' : F]$.

Approches de la « théorie de Galois »

1) *Utilisation d'un élément primitif*

2) *Lemme d'Artin*

3) *Lemme de Dedekind et descente galoisienne*

Depuis le livre d'Artin, la seconde approche est la plus fréquente. La troisième ne figure apparemment que dans Bourbaki et Douady et n'a donc pas vraiment été suivie dans des ouvrages d'enseignement.

Applications de la théorie de Galois

Presque tous les cours ou ouvrages de théorie de Galois étudient les deux problèmes classiques suivants.

- *constructions à la règle et au compas* et *cyclotomie*
- *résolution par radicaux* — mais le théorème de Galois sur les équations résolubles de degré premier n'est que rarement traité ;

Exception notable : Bourbaki, ainsi que la première édition de livre d'Artin !

Certains discutent aussi

- le *théorème fondamental de l'algèbre ;*
- des notions de *calcul* des groupes de Galois, soit par la discussion de résolvantes, soit par l'énoncé du théorème de Tchebotareff.

Apparemment, seuls Bourbaki et Douady utilisent

- la notion d'*algèbre étale*.

Applications de la théorie de Galois

Presque tous les cours ou ouvrages de théorie de Galois étudient les deux problèmes classiques suivants.

- *constructions à la règle et au compas* et *cyclotomie*
- *résolution par radicaux* — mais le théorème de Galois sur les équations résolubles de degré premier n'est que rarement traité ;

Exception notable : Bourbaki, ainsi que la première édition de livre d'Artin !
Certains discutent aussi

- le *théorème fondamental de l'algèbre ;*
- des notions de *calcul* des groupes de Galois, soit par la discussion de résolvantes, soit par l'énoncé du théorème de Tchebotareff.

Apparemment, seuls Bourbaki et Douady utilisent

- la notion d'*algèbre étale*.

Applications de la théorie de Galois

Presque tous les cours ou ouvrages de théorie de Galois étudient les deux problèmes classiques suivants.

- *constructions à la règle et au compas* et *cyclotomie*
- *résolution par radicaux* — mais le théorème de Galois sur les équations résolubles de degré premier n'est que rarement traité ;

Exception notable : Bourbaki, ainsi que la première édition de livre d'Artin !
Certains discutent aussi

- le *théorème fondamental de l'algèbre ;*
- des notions de *calcul* des groupes de Galois, soit par la discussion de résolvantes, soit par l'énoncé du théorème de Tchebotareff.

Apparemment, seuls Bourbaki et Douady utilisent

- la notion d'*algèbre étale*.

Difficultés de l’enseignement de la « théorie de Galois »

1) **Construction** des extensions de décomposition ; l’existence et l’« unicité » de la **clôture algébrique** d’un corps sont souvent évoquées mais le recours nécessaire à l’axiome du choix justifie souvent l’omission de la preuve. Noter que les cours d’un niveau similaire de topologie construisent le revêtement universel d’un espace topologique raisonnable.

Difficultés de l’enseignement de la « théorie de Galois »

1) **Construction** des extensions de décomposition, **clôture algébrique**

2) Méconnaissance de la **théorie des groupes** : pour beaucoup d’étudiants, la correspondance de Galois est une bijection entre deux mondes tout aussi mystérieux l’un que l’autre. Les notions de résolubilité (voire de simplicité) ne sont pas acquises. L’absence de familiarité avec les quotients ne facilite pas les inévitables dévissages.

Difficultés de l’enseignement de la « théorie de Galois »

1) **Construction** des extensions de décomposition, **clôture algébrique**

2) **Théorie des groupes**

3) Difficulté des **exemples concrets**. Presque par définition, la nature du groupe de Galois dépend de l’existence de solutions dans le corps de base de certaines équations auxiliaires ; en ce sens, c’est une *théorie arithmétique* et non *algébrique*.
Pour faire le moindre calcul, il faut savoir décider de l’irréductibilité, de l’existence de racines, etc. dans le corps de base.
Cela pose des problèmes calculatoires, et des problèmes théoriques (critères d’irréductibilité ; notion d’anneau factoriel, ...).

La théorie de Galois : un *apprentissage*

Gilles **Châtelet**, « De la victoire de Platon »,
Gazette des mathématiciens **74**, p. 13–17, octobre 1997.

« On peut comprendre la théorie de Galois comme *apprentissage*, celui du discernement progressif des racines, les conditions formelles d'un tel discernement portant sur des séquences de réduction, et les formules explicites de résolution devenant subsidiaires. Porter tout l'effort de recherche sur les séquences de groupes, de fibrés, de "faisceaux", etc., capables de saisir au vol *le geste même de l'apprendre. . .* telle serait selon Grothendieck, l'inoubliable leçon de Galois. »