Troisième leçon de maths modernes :
LA THÉORIE ALGÉBRIQUE DES GROUPES PAR GALOIS (1830)

(5 décembre 2021)

ARGUMENTAIRE **3**
Problématisation ***3***
Portée intellectuelle ***4***
Algèbre ***4***
PLAN DE LA LEÇON **6**
I – PROBLÉMATISATION À PARTIR DE L'ALGÈBRE CLASSIQUE **7**
Constitution de l'équation algébrique ***7***
Problème algébrique classique ***8***
Exemples 8
Principaux résultats classiques ***8***
Butée, désespoir et perte de confiance ***9***
Lagrange (1781) 9
Cauchy (1811) 9
Parsifal ! 9
Abel ***9***
Exemples d'équations quintiques irrésolubles 9
Dualité 11
« Ne pas être résoluble » ≠ « être irrésoluble » ***11***
Note sur les irrationnels 11
Renversement galoisien ***11***
II – GALOIS ET L'ALGÈBRE MODERNE **13**
Intuition première ***13***
Comment les racines se trouvent-elles groupées par l'équation ? ***13***
Un exemple 13
Relations coefficients-racines 14
Les groupes de Galois ***14***
Les permutations forment un groupe. 15
Le groupe de Galois 15
Théorème de Galois 15
Correspondance de Galois entre corps et groupes via les polynômes ***16***
Idée princeps 16
Extensions de corps et réduction de groupes 16
Le théorème fondamental de la théorie de Galois [TG] ***17***
Corollaire sur l'équation quintique 17
III - PORTÉE INTELLECTUELLE **18**
1. Les pluriels dans les langues vernaculaires… ***18***

2. De la réduplication dans la dialectique intrinsèque/extrinsèque… 18
3. L'inconscient algébrique dont l'inconnue est le symptôme… 19
Métaphore sauvage… 20
4. Le secret de l'algèbre 20
5. Point pour nous le plus important : une conception proprement moderne de l'organisation 21
En mathématiques 21
En musique 21
En politique 22
PETITE DOCUMENTATION 24
Théorie galoisienne des groupes 24
Sur Évariste Galois 24
mamuphi 24
Yves André 24
François Nicolas 24
ANNEXE PLUS MATHÉMATIQUE SUR LA THÉORIE DE GALOIS 26
Logique générale du parcours 26
I - Théorème général 26
La dynamique de décomposition des polynômes 27
La dynamique extensive des corps 27
La dynamique réductrice des groupes 28
Le crantage 28
[Arithmétique de nombres] 28
Extensions L:K 28
K-espace vectoriel 28
Loi de la tour 29
Adjonctions 29
Corps de rupture 29
Corps de décomposition (*splitting* fields) 29
Normalité 29
Clôtures normales 29
[Algèbre de groupes] 29
Groupes 29
Réduction de groupes 29
II - Corollaire spécifique pour l'équation quintique 31
Groupes alternés 31
A_5 31
CORRECTIF : BREF RETOUR SUR LA LEÇON PRÉCÉDENTE (COUPURES DE DEDEKIND) 32

ARGUMENTAIRE

Problématisation

Au début du XIX° siècle, la situation de l'algèbre se trouve bloquée : on ne sait toujours pas résoudre algébriquement (par radicaux [1]) l'équation algébrique (polynomiale) du cinquième degré [2], c'est-à-dire identifier algébriquement chacune de ses cinq racines.
En 1824, Abel vient aggraver la situation en la verrouillant : il démontre (par l'absurde) qu'il est impossible, dans le cas général, de la résoudre.
L'impasse de l'algèbre classique, fondée sur la résolution de son objet propre (l'équation algébrique) devient ainsi totale : à quoi bon désormais une algèbre, travaillant depuis un millénaire (IX°-XVIII°) sur l'objet qu'elle a inventé (*l'équation polynomiale*) - ajouté aux antiques objets arithmétique (*le nombre*) et géométrique (*la figure*) - si l'inconnue n'est plus identifiable par les moyens même (algébriques et arithmétiques) qui l'ont déterminée comme inconnue ? À quoi bon une inconnue déterminée s'il est assuré qu'en algèbre, elle restera radicalement inidentifiable, dépourvue de tout nom propre et donc algébriquement anonyme ?
C'est en ce point qu'en 1830 Galois vient révolutionner la problématique de l'algèbre en dégageant la structure secrète qui préside à cette impossibilité : celle de *groupe*.
Ce faisant, la nouvelle théorie galoisienne inaugure l'algèbre moderne qui va révolutionner l'algèbre classique de trois manières intriquées : 1) en *déplaçant* l'intérêt algébrique porté à l'équation : il faut abandonner le désir de la résoudre et s'attacher désormais à caractériser son groupe, organisateur secret du collectif des racines ; 2) en *étendant* l'algèbre à l'étude de structures telles celle de groupe, sans se restreindre à l'étude des équations polynomiales ; 3) en *reconstruisant* toute la mathématique moderne sur la base de nouvelles structures algébriques (groupes, anneaux, corps, espaces vectoriels, …).
Le statut de l'inconnue x au principe de l'algèbre s'en trouve radicalement renversé : avec sa lettre « x », l'algèbre classique avait formalisé l'objet « inconnue » qu'elle avait extrait de son néant arithmétique (l'arithmétique, opérant du connu au connu, ne connaissait pas l'inconnue) aux fins de le résorber, par calculs successifs, jusqu'à connaître algébriquement *in fine* la quantité inconnue et pouvoir lui donner un nom algébrique.
L'algèbre moderne ne va plus saisir cette inconnue x comme quantité à connaître mais comme index générique affirmant l'existence secrète d'une structure constituante (le groupe de Galois de l'équation). Ainsi, tout de même que la conception moderne d'un secret l'arrache à son acception infantile (une dissimulation volontaire) pour y saisir l'affirmation d'un repli intrinsèque autorisant qu'« *un secret avoué reste bien un secret* » [3] (Lacan), tout de même une longue série de notions, formulées négativement ou privativement dans l'ère classique, vont être rehaussées, par les pensées modernes, au statut positif de propriétés affirmatives :

- avec Dedekind, *l'irrationnel* ne sera plus l'exception numérique (telle $\sqrt{2}$) qui échappe à la mesure rationnelle commune mais deviendra la norme hégémonique de la nouvelle numéricité ;
- avec Lobatchevski, le *non-euclidien* ne relèvera plus de la pathologie spatiale mais deviendra la règle, restreignant rétroactivement l'euclidien au stade de géométrie « primitive » ;
- avec Cantor et Dedekind, *l'infini* ne sera plus l'envers négatif et inaccessible du fini mais l'attribut positif foisonnant de quantités telles qu'une stricte partie peut y équivaloir au tout ;
- avec Hamilton (algèbre) comme avec Connes (géométrie), *le non-commutatif* ne se présentera

---

[1] La formulation d'une racine par radicaux (c'est-à-dire par les symboles $\sqrt{\ }$ ou $\sqrt[n]{\ }$, tels $\sqrt{2}$ ou $\sqrt[3]{7}$) équivaut à sa nomination algébrique. Par exemple, les deux racines de l'équation $ax^2+bx+c=0$ peuvent être formulées par radicaux (c'est-à-dire algébriquement nommées) ainsi : $x = \frac{-b \pm \sqrt{b^2-4ac}}{2a}$.
Ce faisant, on distingue la nomination *algébrique* d'autres formes mathématiques de nomination, par exemple d'une nomination *analytique* (telle celle qu'on peut faire par fonctions elliptiques) : la première est intrinsèque à l'algèbre, les secondes lui sont extrinsèques.
[2] de forme générale $ax^5+bx^4+cx^3+dx^2+ex+f=0$ avec {a, b, c, d, e, f} des nombres rationnels.
[3] Révélant qu'il y a un secret sans pour autant dénouer ce qui fait ce secret, l'aveu défait non le secret mais sa réduplication : on sait désormais qu'il y a un insu.

plus comme un défaut mais comme le socle constituant de nouvelles propriétés algébriques ou géométriques ;
- avec Klein, *l'invariant* ne sera plus le déchet inerte de vivantes variations mais le point autour duquel se constituent les différentes géométries, chacune se mesurant désormais à ce qu'elle préserve plutôt qu'à ce qu'elle modifie ;
- avec Gödel, *l'indécidable* ne sera plus un reste non-calculable mais délimitera le lieu exact où il devient requis de décider ;
- avec Cohen, *l'indiscernable* pointera moins un défaut de constructibilité qu'une puissance générique de type nouveau ;
- avec Hironaka, *l'irrégulier* ne se réduira plus à l'exception d'une pathologie phénoménale mais deviendra singularité locale concentrant les contradictions globales de la situation ;
- avec Robinson et Conway, *l'infinitésimal* ne sera plus cette poussière brownienne que Newton et Leibniz ne savaient canaliser mais deviendra la matière même d'un univers numérique en expansion inouïe ;
- avec Freud, *l'inconscient* ne sera plus ce qui échappe à la conscience mais ce qui structure, selon ses lois propres, la vie subjective des corps parlants ;
- avec Marx, les prolétaires *dépourvus* de tout ce qui n'est pas leurs bras ne seront plus des victimes du capitalisme mais les porteurs d'un projet universel d'émancipation politique ;
- avec Schoenberg, *l'atonal* ne sera plus confiné dans un geste soustractif pour s'affirmer comme nouvelle construction (dodécaphonique) du discours musical ;
- et tout de même avec Galois, *l'inconnu* ne sera plus ce qu'il s'agit de connaître mais ce qui, à raison même d'un incognito assumé, indexe une puissance affirmative de solidarité résistant au classique « diviser pour régner ».

Où l'on mesure que la modernité, loin d'être une déconstruction, tire sa force de retourner la critique du classicisme en une explosion d'affirmations neuves.

Portée intellectuelle

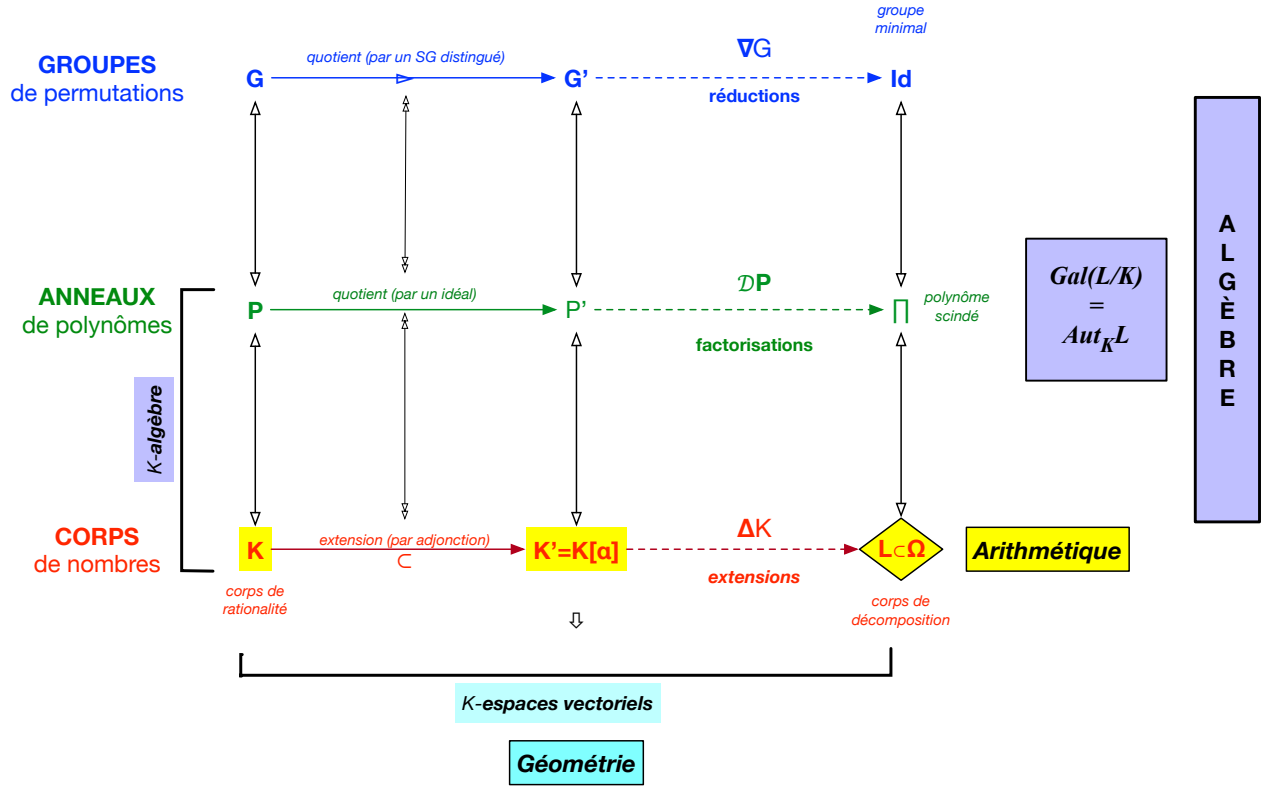
Le propos général de ce cours sera d'introduire à l'algèbre détaillée de cette problématique, en sorte par exemple de comprendre pourquoi les cinq racines réelles de l'équation $x^5+x^4-4x^3-3x^2+3x+1=0$ resteront à jamais algébriquement clandestines, opposant une pseudonymie résolue à l'injonction de l'algèbre classique : « *Racines, vos papiers !* »

- Un premier enjeu intellectuel sera alors de comprendre pourquoi et comment l'organisation *moderne* d'un collectif procède non de la somme *classique* de diverses compétences individuées (tel le casting d'un spectacle ou la sélection des *Sept Samouraï* dans le film de Kurosawa) mais de la constitution, sur la base d'un point de vue d'ensemble partagé, d'un groupe dont la puissance solidaire repose sur la substituabilité de membres essentiellement égaux et anonymes.
- Un second enjeu intellectuel sera de comprendre comment l'algèbre moderne, réduplicant l'algèbre classique (la résolution de l'inconnue *énoncée* devient assumée comme inconnue d'*énonciation*), vient sceller l'inconnue sur elle-même et par là lui donner le statut d'une sorte d'inconscient mathématique si l'on appelle ici *inconscient* une non-conscience réduplicquée, soit un traitement non-conscient du non-conscient ; en ce point, les analogies du travail algébrique avec celui de l'inconscient psychanalytique pullulent : travail à la lettre, travail aveugle, travail de la conscience réflexive n'épongeant pas le retranchement de l'inconscient…

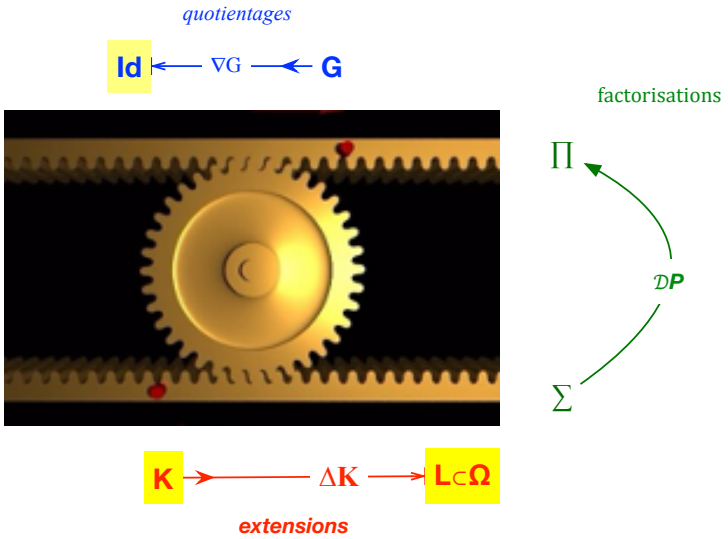
Algèbre

Le pari de cette leçon sera de rendre le mouvement mathématique de cette théorie intelligible à chacun.

Pour ce faire, on montrera comment l'algèbre des polynômes se divise dynamiquement de manière contravariante (c'est-à-dire selon deux ordres inverses) en une arithmétique des nombres et une géométrie des permutations (géométrie formalisée par groupes de Galois), dynamique que l'on peut diagrammatiser ainsi :



On examinera en particulier à quelles conditions le « pignon » polynomial « crante » les deux « crémaillères » contravariantes des *extensions de corps* et des *réductions de groupes* :



PLAN DE LA LEÇON

C'est une gageure d'exposer la théorie de Galois en deux heures, enjeux intellectuels inclus.
Il nous faudra donc faire du fractionné : alterner marche lente et sprints, arrêts sur détails et rapide panorama général, démonstration et intuition, mathématique pure et résonances intellectuelles.

Voici le parcours que je vous propose.

I. Une problématisation : les enjeux mathématiques et intellectuels mobilisateurs, motivant notre objet du jour, la théorie algébrique de Galois.
II. Un examen mathématique de cette théorie en deux parcours :
    a. un lent panorama intuitif ;
    b. un rapide parcours purement mathématique (voir l'annexe) basé sur un vaste diagramme récapitulatif.
III. Quelques enjeux intellectuels, au nombre de cinq.

Et, pour nous donner du cœur au ventre avant d'attaquer cela,

- une petite documentation (cf. fin de ce papier).
- un précédent illustre : fin 1831, Galois crée à 19 ans un *cours public d'algèbre supérieure* à la librairie Caillot (5 rue de la Sorbonne, Paris). Le républicain révolutionnaire qu'il est devenu en 1830 vise ainsi un temps où « *la concurrence, c'est-à-dire l'égoïsme, ne règnera plus dans les sciences, quand on s'associera pour étudier…* ».
- un résultat inédit, le théorème de Goscinny-Uderzo : « *Il existe un groupe de Gaulois irréductible*. »

Disons qu'existe un groupe irréductible de modernes, résistant pieds et poings, corps et âme, à l'empire envahissant du nihilisme postmoderne…

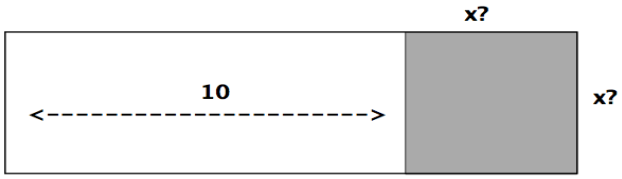
I – PROBLÉMATISATION À PARTIR DE L'ALGÈBRE CLASSIQUE

Constitution de l'équation algébrique

Constitution de l'équation algébrique c'est-à-dire polynomiale à partir d'al-Khawârizmî

Exemple

Un des côtés d'une surface carrée est prolongé de 10 carreaux. La surface du rectangle global ainsi obtenu atteint 39 carreaux. Combien mesurait la surface de départ ?



Solution algébrique (plutôt que géométrique ou arithmétique) : posons x le côté qu'on cherche. Notre problème se résume dans l'équation : $x^2+10x=39$

- Solution aujourd'hui
  $x^2+10x-39=0 \Longrightarrow x=(-10\pm\sqrt{(100+4.39)}/2=(-10\pm\sqrt{256})/2=-5\pm8\Longrightarrow\{3, -13\}\Longrightarrow 3$!
- Solution à l'époque
  Ajouter 25 des deux côtés et transformer ainsi l'équation en une autre :
  $$x^2+10x=39 \Rightarrow x^2+10x+25=64$$
  Or $x^2+10x+25=64$ peut se réécrire ainsi $(x+5)^2=8^2$
  Donc $x+5=8 \Rightarrow x=3$

L'équation algébrique formalise les relations connues qu'une quantité inconnue x entretient avec elle-même (x^n) et avec des quantités connues (nombres rationnels).

Logique de l'inconnue : connaître les relations constituant l'inconnue ; induire l'objet par ses relations (cf. en théorie des catégories le lemme de Yoneda !).

Théorie formelle des équations algébriques, dès Al-Khawârizmî (voir Roshdi Rasched) selon leur degré c'est-à-dire selon le degré des relations de l'inconnue à elle-même.
$\Longrightarrow$ la forme de l'équation que je noterai $\sum$

Exemples

- $x-1=0$
- $x^2-3x+2=(x-1)(x-2)=0$
- $x^3-6x^2+11x-6= (x-1)(x-2)(x-3)=0$
- $x^4-10x^3+35x^2-50x+24= (x-1)(x-2)(x-3)(x-4)=0$
- $x^5-15x^4+85x^3-225x^2+274x-120=(x-1)(x-2)(x-3)(x-4)(x-5)=0$
- mais $x^5+x^4-4x^3-3x^2+3x+1=0 \Longrightarrow$???

$\sum_n$ va caractériser n quantités possédant la même propriété individuelle (c'est là le théorème fondamental de l'algèbre).
Résoudre l'équation, c'est déterminer algébriquement (c'est-à-dire par radicaux) chacune de ces quantités c'est-à-dire connaître désormais algébriquement l'inconnue et plus seulement ses relations.
Attention : connaître *algébriquement*, c'est pouvoir nommer la quantité individuelle avec des radicaux. Ce n'est pas la connaître *géométriquement* (comme on connaît $\sqrt{2}$ comme grandeur de la diagonale d'un carré de côté un), la connaître *arithmétiquement* (d'aussi près qu'on veut par un développement décimal : $\sqrt{2}=1,414\ldots$) ou la connaître *analytiquement* (par exemple par les fonctions elliptiques).

Quand on connaît chaque racine, on a $\sum\rightarrow\prod$:
$$\sum a_i x^i \rightarrow \prod(x-\rho_j)$$

Inversement, si on connaît $\{\rho_j\}$, on peut constituer $\prod$ et en déduire par simple calcul algébrique $\sum$.

degré	$\sum a_i x^i=0$	$\prod(x-\rho_j)=0$
1	$x-1=0$	$(x-1)=0$
2	$x^2-3x+2=0$	$(x-1)(x-2)=0$
3	$x^3-6x^2+11x-6=0$	$(x-1)(x-2)(x-3)=0$
4	$x^4-10x^3+35x^2-50x+24=0$	$(x-1)(x-2)(x-3)(x-4)=0$
5	$x^5-15x^4+85x^3-225x^2+274x-120=0$ mais $x^5+x^4-4x^3-3x^2+3x+1=0$	$(x-1)(x-2)(x-3)(x-4)(x-5)=0$ $\Longrightarrow$???

Problème algébrique classique

Comment passer de $\sum$ à $\prod$?

- Peut-on toujours le faire ? Peut-on toujours nommer algébriquement chaque racine ?
- Si on peut le faire, peut-on formuler une réponse générale comme on le fait pour l'équation quadratique générale : $ax^2+bx+c=0 \Longrightarrow x = \frac{-b\pm\sqrt{b^2-4ac}}{2a}$?

La problématique classique vise à établir une carte d'identité algébrique de toutes les racines. Elle interroge l'équation en demandant : « Racines, vos papiers ! »

Exemples

- degré 1 ? Cf. al-Khawârizmî : il faut quand même démontrer que $x-a=0 \Leftrightarrow x=a$! On le fait en ajoutant a des deux côtés de l'équation (comme sur les deux plateaux d'une balance…).
- degré 2 ? Toujours al-Khawârizmî.

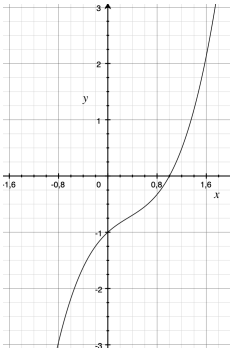
$$ax^2+bx+c=0 \Longrightarrow x = \frac{-b\pm\sqrt{b^2-4ac}}{2a}$$

- degré 3 ? première partie du XVI°
- degré 4 ? seconde partie du XVI°
- degré 5 et plus ?

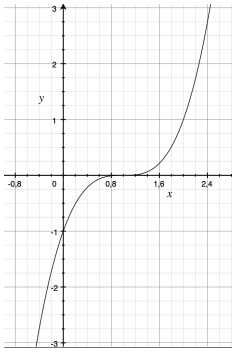
Principaux résultats classiques

- (Théorème fondamental) Pour P_n, il existe toujours n racines complexes et donc pas forcément toutes réelles
  Exemple : $x^3-x^2+x-1=(x-1)(x^2+1)=(x-1)(x-i)(x+i)$
- Bien sûr n racines ne veut pas dire n racines différentes.
  Exemple : $x^3-3x^2+3x-1=(x-1)^3$
- On peut empiriquement le savoir en construisant le graphe de la fonction $y=\sum(x)$
  Par exemple :

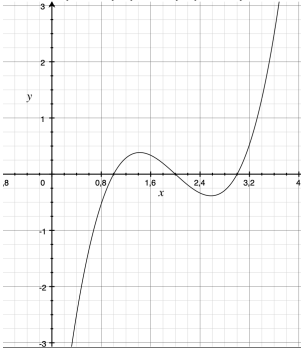
$x^3-x^2+x-1=(x-1)(x-i)(x+i)=0$



$x^3-3x^2+3x-1=(x-1)^3=0$



$x^3-6x^2+11x-6=(x-1)(x-2)(x-3)=0$



- S'il existe des racines complexes, elles vont nécessairement par paires de conjugués.
  En effet $(x-ai)(x-bi)=x^2-(a+b)ix-ab \Longrightarrow a=-b$ pour que i disparaisse $\Longrightarrow x\pm ai$
- S'il existe des racines irrationnelles, elles vont de même être nécessairement groupées (par 2 s'il s'agit de racine carrée, par 3 s'il s'agit de racines cubiques, par n s'il s'agit de racine n ièmes).

En effet $(x-a\sqrt{2})(x-b\sqrt{2})=x^2-(a+b)\sqrt{2}+2ab \Longrightarrow a=-b \Longrightarrow x\pm a\sqrt{2}$

- Les équations de degré inférieur à 5 (linéaires, quadratiques, cubiques, quartiques) sont toutes résolubles par radicaux.

Butée, désespoir et perte de confiance

Question : mais qu'en est-il alors pour les équations cubiques et de degré supérieur ?
Lagrange s'échine – j'indiquerai plus loin sa manière – sans y arriver.
D'où le désespoir et la perte de confiance dans les mathématiques classiques au début du XIX°

Lagrange (1781)

Lettre à d'Alembert du 21 septembre 1781 :

« *Je commence à sentir que ma force d'inertie augmente peu à peu, et je ne réponds pas que je fasse encore de la Géométrie dans dix ans d'ici. Il me semble aussi que la mine est presque déjà trop profonde, et qu'à moins qu'on ne découvre de nouveaux filons, il faudra tôt ou tard l'abandonner. La physique et la chimie offrent maintenant des richesses plus brillantes et d'une exploitation plus facile ; aussi le goût du siècle paraît-il entièrement tourné de ce côté-là, et il n'est pas impossible que les places de la Géométrie dans les Académies ne deviennent un jour ce que sont actuellement les chaires d'arabe dans les Universités*. »

Cauchy (1811)

Discours Sur les limites des connaissances humaines le 14 novembre 1811 à Cherbourg :

« On est tenté de croire que les connaissances de l'homme peuvent croître et se multiplier à l'infini. »

« Cependant si l'on observe que toute notre intelligence et nos moyens sont renfermés entre des limites qu'ils ne peuvent jamais franchir, on se persuadera sans peine que nos connaissances sont bornées comme nos facultés. » [4]

« Que dirais-je des sciences exactes : la plupart paraissent parvenues à leur plus haute période. L'arithmétique, la géométrie, l'algèbre, les mathématiques transcendantes sont des sciences que l'on peut regarder comme terminées, et dont il ne reste plus à faire que d'utiles applications. »

Parsifal !

Posons

I. Lagrange ≡ Amfortas (acte I)
II. Cauchy ≡ Klingsor (acte II)
III. Galois ≡ Parsifal (acte III)

Et, en Prélude de l'acte III : Abel !

Abel

Abel va démontrer par l'absurde que les équations cubiques sont en général irrésolubles.
Bien sûr, certaines sont résolubles.

Exemples :

- $(x-1)^5=x^5-5x^4+10x^3-10x^2+5x-1=0$
- $(x-1)(x-2)(x-3)(x-4)(x-5)=x^5-15x^4+85x^3-225x^2+274x-120=0$

Mais, dans le cas général, elles ne le sont pas.

Exemples d'équations quintiques irrésolubles

Elles peuvent avoir 1, 3 ou 5 racines réelles (puisque les racines complexes vont forcément par paires de conjugués).

---

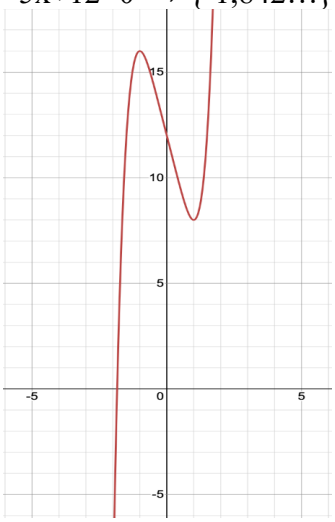
[4] Où l'on retrouve la matrice sophistique du motif contemporain de la finitude : ce qui est borné ne saurait être infini et la limite interdirait l'infini !
Rappelons pourtant que la cardinalité de toute infinité est bornée par la cardinalité de l'ensemble de ses parties, et que l'infinité n'est jamais l'illimité.

(voir polycopié pour de nombreux exemples)

Donnons ici un seul exemple de chaque cas.

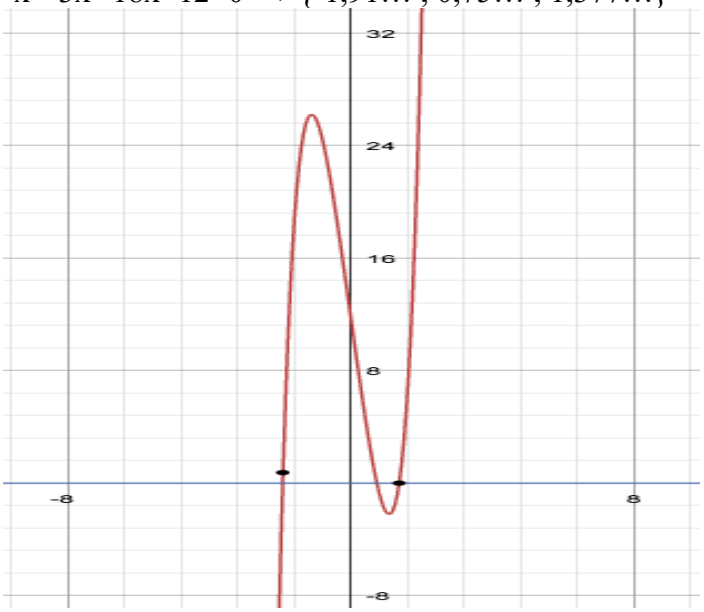
Une racine réelle

$x^5-5x+12=0 \Longrightarrow \{-1{,}842\ldots\}$ [5]



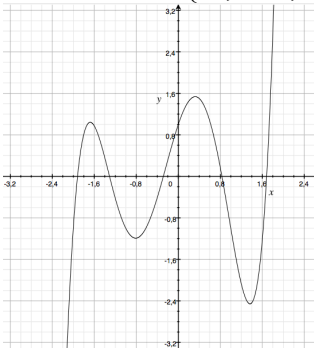
Trois racines réelles

$x^5+3x^3-18x+12=0 \Longrightarrow \{-1{,}91\ldots\ ;\ 0{,}75\ldots\ ;\ 1{,}377\ldots\}$ [6]

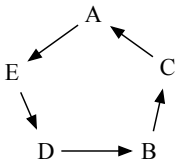


Cinq racines réelles

$x^5+x^4-4x^3-3x^2+3x+1=0 \Longrightarrow \{-1{,}9\ldots\ ;\ -1{,}3\ldots\ ;\ -0{,}2\ldots\ ;\ 0{,}8\ldots\ ;\ 1{,}6\ldots\}$ [7]



$\Longrightarrow$



[5] Cf. Chambert-Loir (p. 129)

[6] Cf. Debarre-Laszlo (VIII.3)

[7] Cf. Alain Connes

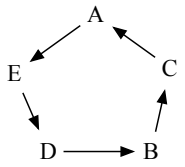
Dualité

- Le groupe *classique* est une *collection constituée* d'*individus indépendants* :

$$\{-2, -1, \frac{1-\sqrt{5}}{2}, 1, \frac{1+\sqrt{5}}{2}\} \Longrightarrow x^5+x^4-4x^3-3x^2+3x+2$$

- Le groupe *moderne* est un *collectif constituant* de *membres solidaires* :

$x^5+x^4-4x^3-3x^2+3x+1 \Longrightarrow$



« Ne pas être résoluble » ≠ « être irrésoluble »

Mais pourquoi telle ou telle équation cubique sera résoluble ou irrésoluble ? La démonstration d'Abel ne le dit pas.

En ce point, ne pas être résoluble n'équivaut pas exactement à être irrésoluble : Abel montre que l'équation cubique ne peut être résolue mais seul Galois va montrer qu'elle est irrésoluble en dégageant la propriété intrinsèque affirmative de l'équation qui rend compte de son irrésolublité.

Cette différence entre la négation (ne pas être résoluble) et l'affirmation (être irrésoluble) est capitale. C'est en un sens la même qu'entre être non fini et être infini (propriété affirmative : une partie stricte peut équivaloir au tout).

Voir plus haut l'argumentaire annonçant cette leçon

Note sur les irrationnels

On a vu, avec Dedekind, l'importance de la différence entre rationnel et irrationnel. Mais, à proprement parler, la démonstration par l'absurde montre que, par exemple, $\sqrt{2}$ n'est pas rationnel sans dégager pour autant la propriété intrinsèque affirmative d'un nombre irrationnel. Il semble que tel soit le cas pour $\sqrt{2}$ depuis l'analyse constructive [8] en particulier de Errett Bishop (1928-1983) [9] mais, à ma connaissance, il n'y a toujours pas de caractérisation affirmative des nombres rationnels (ce qui est beaucoup plus étonnant que la même absence pour les nombres transcendants puisque les algébriques sont dénombrables quand les transcendants ont la puissance du continu).

négation	affirmation
non fini	infini (Dedekind)
non rationnel	irrationnel (?)
non résoluble	irrésoluble (Galois)

C'est donc en ce point où la perspective se renverse d'une négation à une affirmation qu'intervient Galois.

Renversement galoisien

Galois renverse la perspective et opère un retournement dialectique entre aspect principal et aspect secondaire dans l'unité des contraires comme celui qu'a opéré Dedekind entre aspect constituant et aspect constitué.

Je rappelle :

objets→opérations (ou choses→noms), d'où adjonction covariante → adjonction contravariante

à partir de l'extension de l'aspect initialement secondaire.

Ici, ce qui commande, c'est la manière dont l'équation polynomiale groupe des racines selon une propriété individuelle partagée. On va ainsi dégager une propriété commune de type nouveau : une propriété du collectif d'où procèdera une propriété individuelle de type nouveau : être membre d'un groupe. La racine sera ainsi identifiée *génériquement* comme membre d'un groupement donné et

[8] https://fr.wikipedia.org/wiki/Analyse_constructive
[9] https://en.m.wikipedia.org/wiki/Errett_Bishop

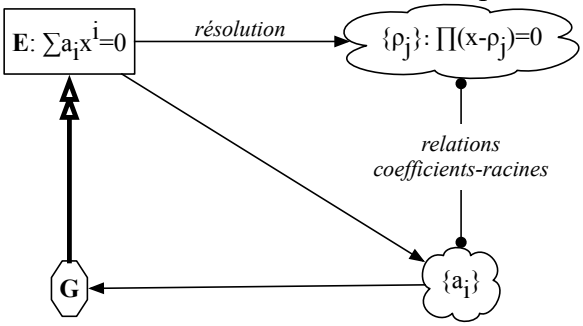
non plus *particulièrement* par son nom algébrique propre :

On passe de équation→résolution individuelle
à résolution individuelle → groupée.
D'où une nouvelle conception de l'équation :
il s'agit de calculer le groupe en question et non plus chaque individu !

Autrement dit, ce qui importe algébriquement, ce n'est plus l'identité (algébrique) des membres mais celle de leur groupement.

On passe d'une **<u>association constituée d'individus</u>** à une **<u>organisation constituante de membres</u>**.

Le pivotement va s'indiquer – voir un peu plus loin – de ce que l'on appelle *les relations coefficients-racines* : les coefficients formalisent en effet les relations primordiales entre les racines.

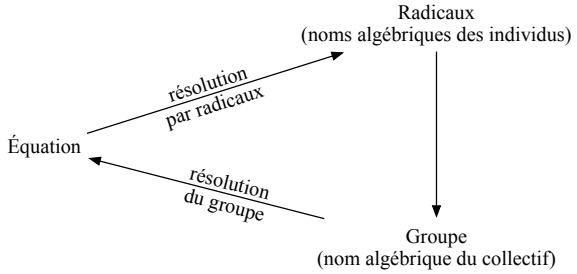


L'irrésolution par radicaux va tenir à l'existence implicite d'un groupement non désolidarisable.

À nouveau, ce retournement affirmatif des modernités : <u>l'irrésolution</u> par radicaux <u>correspond à la résolution</u> d'un vrai groupement solidaire.

A contrario, la résolution par radicaux correspond à la dispersion du groupement, à sa pulvérisation individualiste.

Soit une promotion affirmative de l'inconnu : l'inconnu est la base pour affirmer un groupe !



***

Voyons maintenant, en un lent panorama intuitif, comment la théorie de Galois va clarifier tout ceci.

II – GALOIS ET L'ALGÈBRE MODERNE

Intuition première

L'intuition première va être de voir l'équation algébrique comme le nom propre d'un groupement, d'une organisation constituante.

> Un peu comme Marx et Engels ont vu 18 ans plus tard, dans *Le manifeste du parti communiste*, l'organisation politique comme unifiant ceux qui mettent au poste de commandement politique le point de vue d'ensemble de toute l'humanité.

En quelque sorte, ∑ détermine le pgcd des membres du groupe !
Tout le point est alors de savoir comment ce pgcd groupe les membres d'un groupe et pas seulement les collectionne : il ne les rassemble pas forcément comme le fait une association constituée par récollection d'individus préalablement identifiés – d'où une liste ∏ d'adhérents nominatifs. Un groupe va privilégier la participation individuelle incognito et sous pseudonyme.

> Exemple : les 5 racines réelles anonymes {A, B, C, D, E} de $x^5+x^4-4x^3-3x^2+3x+1=0$.

Donc la résolubilité de l'équation va dépendre du mode de groupement des racines :

- mode associatif : le pgcd est décomposable en répartition des fonctions et des compétences (président, vice-président, secrétaire, trésorier, chargé de communication…) en sous-groupes (conseil d'administration ; diverses commissions spécialisées…) ;
- mode « unifié » : pgcd indécomposable en division interne du travail instituée.

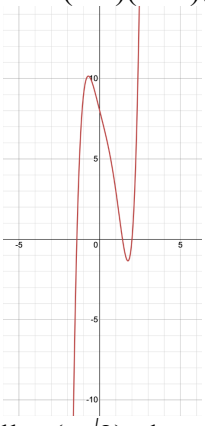
Algébriquement, cela revient à se demander si le groupe est ou non décomposable en sous-groupes car la résolubilité de l'équation va s'avérer dépendre étroitement de la résolubilité du groupe.

Comment les racines se trouvent-elles groupées par l'équation ?

Comment intuitionner le groupement des racines induit par ∑ ?
Par permutation des racines : en les interchangeant et voyant si le résultat sur telle ou telle fonction varie ou reste constant.

Un exemple

$$x^5-2x^4-4x+8=(x-2)(x^2-2)(x^2+2)=0$$



Une racine rationnelle (2), deux irrationnelles ($\pm\sqrt{2}$), deux imaginaires ($\pm i\sqrt{2}$) : {2, $\pm\sqrt{2}$, $\pm i\sqrt{2}$}

$$(x-2)(x^2-2)(x^2+2)=(x-2)(x-\sqrt{2})(x+\sqrt{2})(x-i\sqrt{2})(x+i\sqrt{2})$$

Soit les 5 racines $\{\rho_j\}=\{2 ; a, b ; \alpha, \beta\}$ soit le regroupement suivant : {2}, {a, b}, {α, β}

$$\begin{matrix} 2 \\ a \text{ — } b \\ \alpha \text{ — } \beta \end{matrix}$$

Soient alors les trois fonctions

- $f(x-2)=(x-2)^2+(x-2)+2=x^2-3x+4$
- $g(x^2-2)= (x^2-2)^2+(x^2-2)+2=x^4-3x^2+4$
- $h(x^2+2)=(x^2+2)^2+(x^2+2)+2=x^4+5x^2+8$

Elles seront des fonctions caractéristiques de chacun des trois sous-groupes en ceci que, si l'on permute les racines d'un même sous-groupe, ces fonctions ne varieront pas :

- $f(2)\neq f(a)\neq f(b)\neq f(\alpha)\neq f(\beta)$
- $g(a)=g(b)$ mais $\neq g(2)\neq g(\alpha)\neq g(\beta)$
- $h(\alpha)=h(\beta)$ mais $\neq g(2)\neq g(a)\neq g(b)$

Relations coefficients-racines

En ce point, remarquons qu'il existe déjà n fonctions caractéristiques des n racines d'une équation de degré n : les coefficients de l'équation !

d°	$\sum$	$\prod$	$\sum\prod$
1	$x+a=0$	$(x-p)=0$	x $-p=0$
2	$x^2+ax+b=0$	$(x-p)(x-q)=0$	x^2 $-(p+q)x$ $+pq=0$
3	$x^3+ax^2+bx+c=0$	$(x-p)(x-q)(x-r)=0$	x^3 $-(p+q+r)x^2$ $+(pq+qr+rp)x$ $-pqr=0$
4	$x^4+ax^3+bx^2+cx+d=0$	$(x-p)(x-q)(x-r)(x-s)=0$	x^4 $-(p+q+r+s)x^3$ $+(pq+qr+rs+sp)x^2$ $-(pqr+qrs+rsp+spq)x$ $+pqrs = 0$
5	$x^5+ax^4+bx^3+c^2x+dx+e=0$	$(x-p)(x-q)(x-r)(x-s)(x-t)=0$	x^5 $-(p+q+r+s+t)x^4$ $+(pq+qr+rs+st+tp)x^3$ $-(pqr+qrs+rst+stp+tpq)x^2$ $+(pqrs+qrst+rstp+stpq+tpqs)x$ $-pqrst=0$

Forme générale :

$$\sum_{i=1}^{n} a_i x^i = x^n - \left(\sum_{j=1}^{n} \rho_i\right) x^{n-1} + \cdots + (-1)^n \prod_{j=1}^{n} \rho_j$$

Peut-on alors construire d'autres fonctions qui nous permettront d'individualiser les racines ?
Telle a été la voie explorée par Lagrange à partir de la fin du XVIII°.

Cette voie a été une impasse : pour avancer, il fallait remonter de la fonction caractéristique au groupe qu'elle caractérisait implicitement.

Les groupes de Galois

Que veut dire que les racines sont groupées ?
Cela veut dire que, dans un corps de résolution donné (c'est-à-dire dans un système donné d'identification des nombres : par exemple celui des nombres rationnels, ou des nombres réels, ou des complexes), on peut permuter certaines racines sans qu'on ne puisse rien y voir par les moyens algébriques intrinsèques du corps en question c'est-à-dire par toute expression algébrique construite sur ce corps.

Ainsi sur $\mathbb{Q}$, $f(x) = x^2-2$ constitue une expression algébrique où $\pm\sqrt{2}$ sont permutables puisque $f(\pm\sqrt{2})=0$. De même bien sûr pour $(x^2-2)^2+(x^2-2)+4$ ou tout autre expression algébrique de même acabit.

Les permutations forment un groupe.

Ce que l'on va alors grouper, ce seront les opérations de permutation entre les racines.
En effet, on peut les combiner entre elles : on obtient toujours des permutations.

- La succession de deux permutations est une permutation.
- Il y a une permutation neutre dite *Identité* : celle où aucune racine ne change de place !
- Toute permutation a une permutation inverse telle que la succession d'une permutation et de son inverse ramène au point de départ, c'est-à-dire soit la permutation *Identité*.
- Si l'ordre de succession n'importe pas – on dit alors que les permutations peuvent commuter -, alors le groupe sera dit commutatif ou abélien (en hommage à Abel).

Le groupe de Galois

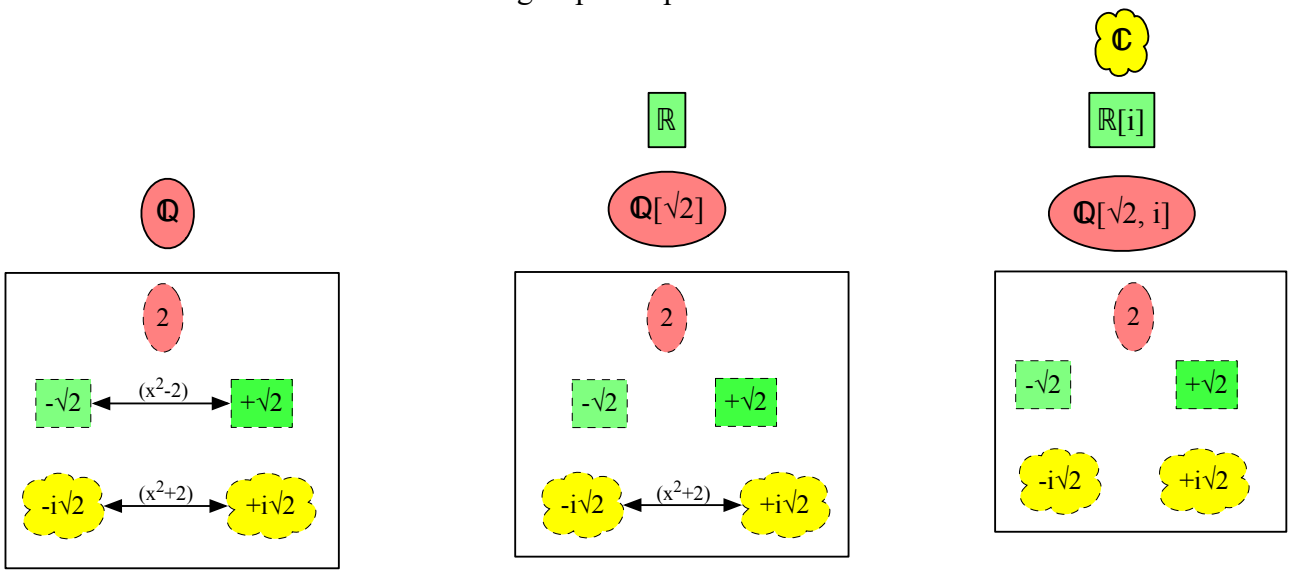
Le GG d'une équation est le groupe des permutations entre les racines (sur un corps donné !) qui laissent invariantes toutes les expressions rationnelles de ces racines.

Exemple

$$x^5-2x^4-4x+8=0$$

- Sur $\mathbb{Q}$, on a $x^5-2x^4-4x+8=(x-2)(x^2-2)(x^2+2)$
- Sur $\mathbb{R}$ ou plus restrictivement sur $\mathbb{Q}[\sqrt{2}]$, on a $x^5-2x^4-4x+8=(x-2)(x-\sqrt{2})(x+\sqrt{2})(x^2+2)$
- Sur $\mathbb{C}$, ou plus restrictivement sur $\mathbb{Q}[\sqrt{2}, i]$, on a $x^5-2x^4-4x+8=(x-2)(x-\sqrt{2})(x+\sqrt{2})(x-i\sqrt{2})(x+i\sqrt{2})$

Les groupes respectifs sont :



Théorème de Galois

Galois va démontrer que l'équation algébrique est résoluble si son groupe de Galois l'est c'est-à-dire s'il est décomposable en une série de sous-groupes emboîtés.

Ce faisant, il va dégager la raison théorique sous-jacente du théorème d'Abel.

Point remarquable : il va le faire sans pour autant proposer une manière pratique de déterminer (d'identifier, de nommer) le groupe spécifique d'une équation donnée.

Cf. puissance de la formalisation !

D'où les points suivants :

- À tout ∑ un G qu'on appelle son groupe de Galois [GG].
- Si G est résoluble (je noterai ∇G [10] le processus de résolution), alors ∑→∏
- Que veut dire que G soit résoluble ?

Galois va caractériser le processus général de résolution par une correspondance qui va s'appeler la correspondance de Galois [CG] entre ∇G et une extension du corps K de définition des racines que je noterai ΔK.

---

[10] Le signe ∇ ne désigne pas ici l'opérateur « nabla » mais correspond simplement au signe delta Δ renversé.

Correspondance de Galois entre corps et groupes via les polynômes

Idée princeps

C'est l'idée que la résolution algébrique dépend étroitement du corps caractérisant les racines, c'est-à-dire des moyens algébriques mobilisés pour nommer les racines.

La résolution est donc relative à un corps :

- $x^2+3x+2=0$ n'est pas résoluble sur $\mathbb{N}$ car$\{-1, -2\}\notin\mathbb{N}$ mais $\in\mathbb{Z}$: $x^2+3x+2=(x+1)(x+2)$.
  Par contre l'équation est résoluble sur $\mathbb{Z}$.
- $4x^2-1=0$ n'est pas résoluble sur $\mathbb{Z}$ car $\pm1/2\notin\mathbb{Z}$ mais $\in\mathbb{Q}$: $4x^2-1=(x-1/2)(x+1/2)$
  Par contre l'équation est résoluble sur $\mathbb{Q}$.
- $x^2-2=0$ n'est pas résoluble sur $\mathbb{Q}$ car $\pm\sqrt{2}\notin\mathbb{Q}$ mais $\in\mathbb{R}$: $x^2-2=(x-\sqrt{2})(x+\sqrt{2})$
  Par contre l'équation est résoluble sur $\mathbb{R}$ mais aussi sur $\mathbb{Q}\oplus\{\pm\sqrt{2}\}$ noté $\mathbb{Q}[\sqrt{2}]$.
- $x^2+4=0$ n'est pas résoluble sur $\mathbb{R}$ car $\pm2\sqrt{(-1)}=2i\notin\mathbb{R}$ mais $\in\mathbb{C}$: $x^2+4=(x-2i)(x+2i)$
  Par contre l'équation est résoluble sur $\mathbb{C}$ mais aussi sur $\mathbb{R}\oplus\{\pm2i\}$ noté $\mathbb{R}[i]$.

Dans ces quatre cas, le groupe des deux racines n'est pas séparable sur le corps considéré.
D'où l'idée qu'une extension de domaine, telles $\mathbb{N}\to\mathbb{Z}\to\mathbb{Q}\to\mathbb{R}\to\mathbb{C}$, va correspondre à une possible décomposition du groupe $\Longrightarrow$ la « correspondance de Galois » : $\Delta K\to\nabla G$.

Noter que $\mathbb{C}$ atteint, on ne peut étendre algébriquement car $\mathbb{C}$ est algébriquement clos.

Galois, voyant que de telles extensions massives changent radicalement la donne pour la résolubilité, va imaginer des extensions plus circonscrites et étroitement ajustées à notre problème algébrique.

Ce faisant, Galois va être celui qui invente les deux notions décisives d'adjonction et d'extension : il invente l'extension de corps par adjonction d'un élément (et non pas d'une opération comme on l'a vu avec Dedekind).

Exemple

Extension de $\mathbb{Q}$ par adjonction de $\sqrt{2}$: $\{p+q\sqrt{2}\}$ qu'on note $\mathbb{Q}[\sqrt{2}]$.
$\Longrightarrow x^2+2=(x-\sqrt{2})(x+\sqrt{2})$ qui est résoluble sur $\mathbb{Q}[\sqrt{2}]$
Ainsi $\Delta K\ (+\sqrt{2})\Longrightarrow\nabla G\ (2G_2$ avec $G_2=\{\sqrt{2}\})$

Extensions de corps et réduction de groupes

$\nabla G/\Delta K$

Détaillons la mécanique par l'image d'une crémaillère.

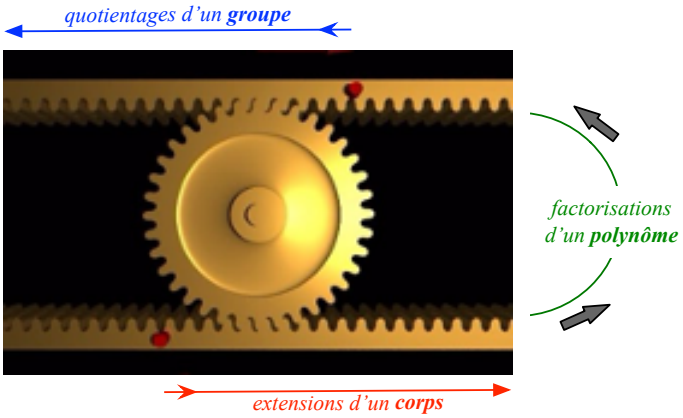
Crémaillère

Le « pignon » polynomial va « cranter » deux « crémaillères » contravariantes [11] : celle des *extensions de corps* et celle des *réductions de groupes* :

[11] *Covariance* et *contravariance* peuvent être intuitionnées ainsi :

- tendez un bras horizontalement en le dirigeant face à vous ; si vous pivotez sur vous-même, votre bras pivotera comme votre corps : sa rotation sera *covariante* à celle de votre corps ;
- maintenant, tendez votre bras horizontalement en attrapant, comme dans le métro, une barre verticale immobile ; si vous pivotez sur vous-même, votre bras cette fois tournera dans le sens inverse de votre corps : sa rotation sera *contravariante* à celle de votre corps.

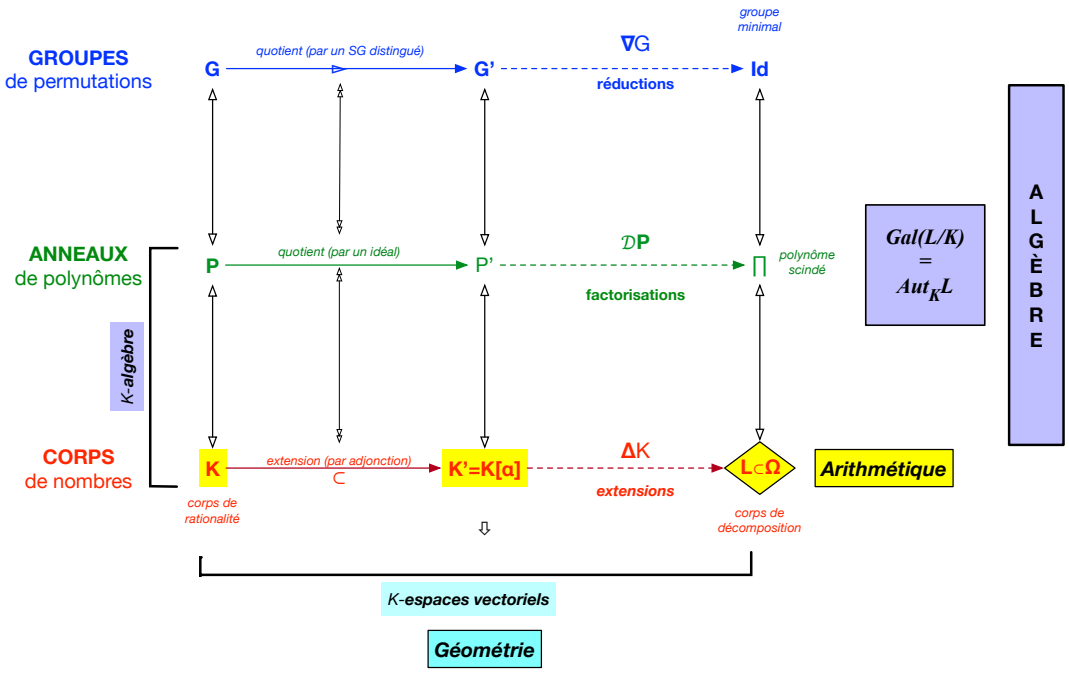
Résolution d'une **équation** algébrique



[vidéo : https://www.youtube.com/watch?v=EjiIcqmtEuo]

Tableau synthétique

L'algèbre des polynômes va ainsi se diviser dynamiquement de manière contravariante (c'est-à-dire selon deux ordres inverses) en une arithmétique des nombres (formalisée en corps) et une géométrie des permutations (géométrie formalisée par groupes de Galois), dynamique que l'on peut diagrammatiser ainsi :



Le théorème fondamental de la théorie de Galois [TG]

Une équation algébrique est résoluble ssi le GG de permutations de ses racines est résoluble.

Corollaire sur l'équation quintique

L'équation quintique générale n'est pas résoluble (et donc également l'équation générale de degré n avec n>5) car son GG ne l'est pas.

Pourquoi le GG de l'équation quintique n'est-il pas en général résoluble ?

Car il est simple et non abélien (et Galois démontre qu'un groupe simple, pour être résoluble, doit être abélien).

Et pourquoi le GG de l'équation quintique est-il en général simple et non abélien ?

Parce que tout G_n (pour $n \geq 5$) a un sous-groupe alterné A_5 lequel est simple et non abélien.

Pour un examen mathématique plus détaillé, voir annexe.

***

III - PORTÉE INTELLECTUELLE

Thématisons la portée intellectuelle considérable de cette théorie de Galois en cinq directions :

1) le pluriel dans les langues vernaculaires ;
2) la réduplication dans la dialectique intrinsèque/extrinsèque ;
3) l'inconscient algébrique dont l'inconnue est le symptôme ;
4) le secret de l'algèbre ;
5) une conception proprement moderne de l'organisation.

1. Les pluriels dans les langues vernaculaires…

Tout ceci nous apprend que la langue algébrique des polynômes distingue *singulier, duel, triel, quadriel, et pluriel*.
Le *Sursurunga* de Papouasie-Nouvelle-Guinée [12] (langue maternelle de seulement 3.000 personnes en 1991) semble la seule langue à mobiliser le jeu complet {singulier, duel, triel, quatriel, paucal (peu), pluriel (beaucoup)}, du moins pour les pronoms.

2. De la réduplication dans la dialectique intrinsèque/extrinsèque…

C'est un point que nous rencontrons ici pour la première fois mais qui va s'avérer décisif dans la modernité mathématique – nous l'examinerons en détail avec Gauss (courbure extrinsèque→ intrinsèque) et Riemann (constitution intrinsèque d'un espace sans nécessité d'un contexte plus général ou d'un environnement).
Ici toute la théorie porte sur le point : une racine algébriquement définie peut-elle être ipso facto algébriquement nommée ?
La réponse est : dans le cas général, non !

> Je rappelle qu'il peut exister des résolutions non algébriques, arithmétiques, géométriques et singulièrement analytiques (avec par exemple les fonctions elliptiques), d'une équation quintique mais de telles résolutions sont extrinsèques à l'algèbre.

L'intrinsèque constitue une figure de l'immanence. Elle consiste à se demander : qu'est-ce qui, dans une situation donnée, y reste accessible selon les moyens employés pour la délimiter ?

> Avec Gauss, ce sera : la courbure d'une surface est-elle accessible par un habitant de la surface ou faut-il, pour la définir, un point de vue extérieur sur la surface, inaccessible à qui est dans la surface ?

Ici, on a la question : la détermination individuelle des racines est-elle accessible par les moyens mêmes qui ont défini ce qui possède des racines ? Est-elle algébrique comme le polynôme est algébrique ?
Peut-on énoncer algébriquement les racines d'un polynôme algébrique ?

> On perçoit comment cette question s'apparente à la réduplication chez Kierkegaard : il s'agit qu'une énonciation algébrique s'accorde à un énoncé algébrique (tout comme, pour Pascal, il s'agit de parler modestement et pas orgueilleusement de la modestie).

Peut-on résoudre algébriquement le problème algébrique de l'équation polynomiale ?

Abel répond que *non* : on ne peut en général résoudre par radicaux l'équation algébrique quintique. On n'a donc pas ici de réduplication car « algébrique » veut dire « par radicaux ».

Galois va répondre *oui* à un problème dérivé : on peut résoudre algébriquement le problème de savoir si telle ou telle équation algébrique donnée est résoluble.
Galois opère ce faisant une extension de ce que *algèbre* veut dire : non plus, comme dans l'algèbre classique, résolution des équations mais mise au jour de leur structure « inconsciente » en groupe.
Autrement dit, si on ne peut résoudre algébriquement une équation algébrique, on peut par contre résoudre algébriquement le problème de la résolubilité !

[12] https://en.wikipedia.org/wiki/Sursurunga_language

Olivier Debarre (Ens-Ulm) nous l'explique très bien :

https://www.youtube.com/watch?v=VBauUSg5Hs0

« *Les mathématiciens du temps de Galois ont considéré que ses critères de résolubilité des équations de degré premier ne constituaient pas une réponse satisfaisante à la question car ces critères nécessitaient de connaître des informations à priori sur les racines. Ils attendaient plutôt un critère général ne faisant intervenir que les coefficients de l'équation et permettant de savoir, par simple inspection de ces coefficients, si l'équation était ou non résoluble par radicaux. La théorie de Galois, très en avance sur son temps, et montrant que le problème était bien plus subtil, ne correspondait pas à ces attentes. Et ce n'est que beaucoup plus tard que le monde mathématique a commencé à réaliser que la théorie de Galois allait bien au-delà du problème, somme toute très artificiel, de la résolution par radicaux des équations algébriques. Galois avait en fait propulsé tout le domaine de l'algèbre dans un nouveau monde : celui des groupes, des extensions de corps, et de bien d'autres concepts fondamentaux des mathématiques d'aujourd'hui. En particulier, de nos jours on s'est rendu compte qu'il est bien plus important de savoir calculer le groupe de Galois d'un polynôme, plutôt que de savoir s'il est résoluble par radicaux.* »

3. L'inconscient algébrique dont l'inconnue est le symptôme…

L'algèbre moderne, réduplicant l'algèbre classique (la résolution de l'inconnue *énoncée* devient assumée comme inconnue d'*énonciation*), vient sceller l'inconnue sur elle-même et par là lui donner le statut d'une sorte d'inconscient mathématique si l'on appelle ici *inconscient* une non-conscience réduplicative, soit un traitement non-conscient du non-conscient ; en ce point, les analogies du travail algébrique avec celui de l'inconscient psychanalytique pullulent : travail à la lettre, travail aveugle, travail de la conscience réflexive n'épongeant pas le retranchement de l'inconscient…

Avec Galois, il y a un retournement de l'algèbre assez homologue à celui que Freud a opéré relativement à la conscience : Galois hérite d'une algèbre ambitionnant de porter à la conscience algébrique tout élément d'un ensemble polynomial algébriquement défini, l'ambition d'une algèbre transparente à elle-même lors même que sa propre raison d'être est de transformer une inconnue x, constituante de l'algèbre, en une quantité connue (un nombre réel ou une grandeur complexe) via des calculs à la lettre et ce faisant très aveugles.

L'algèbre se constitue donc à partir d'une opacité, d'une obscurité : l'inconnue x.

Pour le coup, il est intéressant que le genre féminin affecte cet élément qui résiste à la transparence, à la connaissance intégrale (voir les formules de la sexuation chez Lacan…).

Son hypothèse constituante est que l'inconnue est connaissable via l'équation algébrique qui n'existe que pour ce faire.

- L'algèbre classique devient mélancolique (voir le dépérissement du désir d'algèbre chez Lagrange et Cauchy) quand elle réalise qu'on n'arrivera sans doute jamais à éponger toute inconnue en quantité algébriquement connaissable, qu'il faudra donc se résoudre à admettre que l'algèbre pose des questions auxquelles elle ne peut répondre sur ses propres forces. Et si, dans ce cas, les réponses à ses propres questions lui resteront éternellement inaccessibles, c'est donc devoir admettre que la conscience algébrique est intrinsèquement barrée, limitée, en quelque sorte castrée : un point, au demeurant un point décisif pour elle (la résolution algébrique de son objet propre), lui échappera toujours. Dans ce cas en effet, à quoi bon continuer l'algèbre ?
- L'algèbre moderne renverse le propos : son propos n'est plus la pleine conscience de ses équations, leur intégrale transparence intrinsèque mais la compréhension de ce qui barre cette pleine

conscience, non pour lever cette barre (« pour prendre conscience de ce qui n'était pas conscient ») mais pour prendre mesure des limites de la conscience et par là comprendre (prendre avec soi, pratiquer) la dialectique ici secrètement à l'œuvre.

Voir le point suivant sur « le secret de l'algèbre »…

Autrement dit, et pour nouer ce thème au précédent : l'intrinsèque n'est plus constitué autour du motif de la conscience et de la transparence mais selon le motif d'une discursivité rationnelle sur l'inconscient et l'opaque.

Point ici essentiel à ne pas oublier : Galois démontre qu'il y a groupe mais il ne montre pas le groupe particulier d'une équation donnée – appliquer la théorie de Galois à une équation donnée pour en dégager son groupe de permutations n'est pas une sinécure et nécessite à chaque bois un bricolage ad hoc.

Je ne m'étends pas ici sur ces techniques qui mobilisent aujourd'hui la puissance informatique mais, pour plus de détails, voir le polycopié annexé à cette leçon.

On peut ainsi dire métaphoriquement que la théorie de Galois dispose l'algèbre moderne en théorie de l'inconscient mathématique.

Métaphore sauvage…

Filons sauvagement la métaphore lacanienne en posant que, dans les rapports respectifs de $\prod$, $\sum$ et G, $\prod$ (la liste explicite des racines, devenues algébriquement conscientes) est à la place du *Moi*, $\sum$ (l'équation polynomiale constituante entendue comme question algébrique ouverte, comme subjectivation de l'algèbre) est à la place du *sujet* et G (le groupe constituant, acteur secret structurant l'équation) est à la place de *l'inconscient* :

$$\prod / \sum / G \equiv \textit{Moi / sujet / inconscient} !$$

- Comme *l'inconscient est structuré comme un langage*, le groupement des racines est structuré comme un groupe galoisien.
- Comme *le sujet est inconnu du moi*, le commun des racines est inconnu de leur identification par radicaux.
- Comme *l'inconscient est quelque chose qui parle dans le sujet*, le groupe galoisien est ce qui parle dans l'équation.
- Comme *le sujet ne sait pas avec quoi il parle*, l'équation ne sait pas avec quelle algèbre elle parle.
- Comme *l'inconscient commence à la limite où le sujet se perd*, le groupe commence à la limite où l'équation se perd.
- Comme *l'inconscient est la mémoire de ce que l'homme oublie*, l'algèbre est la mémoire (aveuglément calculatrice) de ce que la mathématique oublie.
- Comme *l'inconscient est un savoir sans que le sujet en soit conscient*, le groupe est un savoir sans que l'équation en soit consciente.
- Comme *l'inconscient est l'insu dont le sujet est absent*, le groupe est l'insu dont l'équation est absente.
- *ad libitum…*

4. Le secret de l'algèbre

L'algèbre, en formalisation la mathématique « à la lettre » (x), la dote d'une puissance de calcul aveugle là où la géométrie interprète la mathématique en mettant en figure l'intuition spatiale.

L'aveuglement du calcul algébrique a souvent été mis en rapport avec l'énigme du temps (voir Hamilton lui-même – l'algèbre comme structure du temps - puis bien d'autres après lui).

L'algèbre devient le secret même de la puissance mathématique car en elle, deux contraires sont rendus « régionalement » indiscernables : le calcul (aveugle) et la raison (éclairante).

Où l'on retrouve alors la profonde vérité de l'aphorisme lacanien : « un secret avoué reste un secret ». Car le secret peut être vu comme un point où énoncé et énonciation deviennent localement indiscernables, ce qui est bien le cas dans l'algèbre moderne : elle pointe en nommant ce qui fait

butée pour la résolution en pleine lumière de l'équation (le groupe) mais pour autant, elle ne porte pas au jour le groupe de chaque équation. Elle énonce qu'« il y a un groupe à l'œuvre » sans pour autant identifier chaque groupe, dans dégager ses papiers d'identité.
L'algèbre moderne abandonne donc profondément le désir classique qui énonce « Racines, vos papiers ! » : ce n'est pas qu'il le transfert à un nouvel objet plus essentiel (« Groupe, tes papiers ! ») mais c'est qu'il révolutionne la problématique d'énonciation elle-même et déplace le désir algébrique : non plus celui d'une identification individuelle mais celui du fonctionnement d'une structure.
Or ici comme ailleurs, ce qui noue le rapport énoncé/énonciation en secret, c'est l'existence d'un désir qui, bien que déclaré, gardera son secret lequel tient à sa puissance dynamique – comme on le voit bien quand quelqu'un avoue son désir sans que pour autant ceci prenne alors pour vous la forme d'un désir équivalent (l'énigme du désir éprouvé par tel ou telle autre…).
Le fait d'énoncer du secret (mon secret, c'est ceci ou cela) ne défait pas le secret de son énonciation : ce qui fait que ceci ou cela est effectivement désirable.

Bref, l'algèbre moderne révolutionne le désir algébrique (voir Debarre) et ce faisant déplace le secret de l'algèbre sans aucunement l'éponger.

5. Point pour nous le plus important : une conception proprement moderne de l'organisation

En mathématiques

Portée immense des GG
L'algèbre va devenir la théorie des structures algébriques et non plus de la résolution des équations polynomiales ⟹ les structures de groupes, d'anneaux, de corps, d'espaces vectoriels, etc.
D'où que l'algèbre moderne va structurer tous les domaines des mathématiques modernes : voir le mouvement d'algébrisation (c'est-à-dire de formalisation algébrique) de la géométrie (géométrie algébrique), de la topologie (topologie algébrique), etc.

En musique

Voir les deux modes d'organisation des hauteurs dans la tonalité et dans le dodécaphonisme.

Organisation tonale des hauteurs

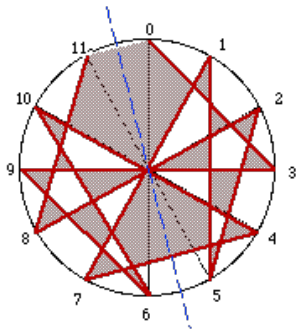
Chaque hauteur d'une tonalité a une carte d'identité individuelle :

- un nom propre :
  I. Tonique
  II.
  III.
  IV. Sous-dominante
  V. Dominante
  VI.
  VII. Sensible
- un prénom : fonction de la modulation par rapport à la tonalité principale (pour un morceau en Mib majeur, le mi bémol sera la tonique de la tonalité principale mais la sous-dominante de la tonalité en Sib majeur).

Organisation dodécaphonique des hauteurs

La série n'existe que comme pure structure d'ordre sur les intervalles entre les hauteurs : les hauteurs absolues deviennent des composantes incognito de la structure sérielle (d'où la difficulté en général de reconstituer les séries utilisées).

{0,3,8,5,11,2,10,1,7,4,9,6}



En politique

D'une **association constituée d'individus** à une **organisation constituante de membres**
⟹ deux conceptions de l'organisation politique :
1) par inscription individuelle (logique étatique) ;
2) par unification subjectivée (logique émancipatrice).

Exemple de la ZAD de Nantes

En avril 2018, pendant plusieurs jours, le conflit politique de Notre-Dame-des-Landes s'est focalisé sur un point symbolique intéressant : les dossiers d'activités alternatives déposés auprès de l'État par les occupants de la ZAD resteraient-ils strictement collectifs (comme le concevaient les intéressés) ou seraient-ils dispersés en projets, individuellement assumés (comme le voulait l'État) ? En bref, l'acteur faisant face à l'État pouvait-il rester un groupe, parfaitement défini par son projet et ses premières réalisations, déterminé par son mode interne de fonctionnement, nommé comme tel mais restant volontairement sans membres individuellement déclarés ou cet acteur, pour être reconnu par l'État, passerait-il nécessairement par une identification individuelle de nature policière (« Vos papiers ! »), le groupe étant ainsi conçu essentiellement composé de cartes individuelles d'identité ?

Voici comment la ligne de partage s'est initialement constituée.

Le Monde, 18 avril 2018

« S'ils viennent (...) pour me dire "on ne donnera pas nos noms", s'ils ne répondent pas a minima à cette demande, le président de la République a été très clair, il y aura de nouveau des expulsions », expliquait la préfète Nicole Klein.
Il pourra y avoir des projets collectifs et autres qu'agricoles, « mais il faut donner son nom », a-t-elle insisté.
« Je trouve ça absolument incompréhensible de ne pas vouloir donner son nom. »
Les occupants lui ont fait parvenir, quelques jours avant le lancement des opérations d'expulsion, une proposition de convention collective englobant environ 500 des 1 650 hectares de la ZAD, mais « il n'y avait pas un seul nom sur le projet », selon la représentante de l'État.
Le choix est désormais clair : ou bien les intéressés consentent à se déclarer nominativement et à déposer une esquisse de leur future activité et ce, avant lundi 23 avril, ou bien les 2 500 gendarmes postés autour de Notre-Dame-des-Landes pourraient recevoir l'ordre de rayer du bocage une majorité des 68 squats restants, après que 29 habitations précaires ont été démolies la semaine passée.
C'est donc l'avenir même de la ZAD qui se joue. La plupart des 250 personnes installées durablement sur ce secteur – vaste de 1 650 hectares – demeurent hors la loi selon l'appréciation de l'Etat. Si l'on excepte quatre agriculteurs historiques qui s'apprêtent à obtenir la rétrocession de leurs terres expropriées, la préfète Nicole Klein ne recense que « 33 conventions d'occupation temporaire de parcelles » paraphées par des personnes dûment identifiées.
Marcel Thébault, un des 4 agriculteurs historiques : « La réalité agricole de la ZAD existe. Mais il est impossible de prédire quelles décisions seront prises. La difficulté pour chacun consiste à se détacher du groupe. » Les militants de base, note-t-il encore,

« ont du mal à comprendre ce refus de procéder à des déclarations individuelles ». « Ne ratons pas la dernière étape, énonce Nicolas Hulot, ministre de la transition écologique. Ne rentrons pas dans une spirale de postures, de confrontations, de violences, ne confondons pas écologie et anarchie. »

Et voici comment, les occupants ont rapidement cédé aux injonctions de l'État.

Le Monde, 21 avril 2018

Une délégation d'occupants de la ZAD a annoncé, vendredi 20 avril, au sortir d'une réunion à la préfecture à Nantes, qu'ils acceptaient de déposer des projets nominatifs comme le demande le gouvernement.

« Nous décidons aujourd'hui de répondre aux injonctions du gouvernement. Nous voulons stopper l'escalade de la tension sur la zone et obtenir enfin le temps nécessaire au dialogue et à la construction du projet que nous défendons » ont-ils dit, en précisant avoir déposé quarante projets nominatifs, parmi lesquels certains individuels et certains collectifs.

La préfète des Pays de la Loire, Nicole Klein, a salué devant les journalistes le travail réalisé :

« Ils ont fait un gros travail, il faut le reconnaître, et ils ont amené une vingtaine de projets nominatifs, donc le nom, une adresse, un projet qu'on va bien sûr examiner de près d'ici lundi soir. »

« C'est un signe de bonne volonté », a dit la représentante de l'Etat, « car ils ont jusqu'à aujourd'hui refusé de donner des projets nominatifs », et maintenant « ils ont donné des projets nominatifs ». « Ils ont répondu en partie à la demande qui était de déposer des projets nominatifs », a précisé Mme Klein.

L'État avait demandé aux occupants de remplir d'ici à lundi soir des formulaires individuels, comportant leur nom et les grandes lignes de leur projet agricole ou paraagricole.

Relevons la particulière modernité de cette ligne de partage : elle rejoint en effet immédiatement le point précis sur lequel la modernité mathématique s'est engagée, il y a maintenant deux siècles de cela : la théorie des groupes par Évariste Galois !

***

PETITE DOCUMENTATION

(pour une documentation détaillée et commentée, voir le polycopié)

Théorie galoisienne des groupes

- Ian Stewart : *Galois Theory* (Chapman & Hall, third Edition ; 2004)
- Emil Artin : *Galois Theory* (1942 ; réédition Dover, 1998)
- J. P. Friedelmeyer : *Émergence du concept de groupe* (Brochure APMEP n°83, 1991)
- Bertao, Cifuentes et Szczeciniarz : *In the steps of Galois* (Hermann, 2014)

Sur Évariste Galois

- Fernando Corbalan : *Galois, l'invention de la théorie des groupes* (RBA, coll. Génies mathématiques ; 2018)
- Alexandre Astruc
    - Une biographie : *Évariste Galois* (Flammarion, 1994)
    - Un film : *Évariste Galois ou l'éloge des mathématiques* (1965) [13]

mamuphi

Yves André

- *Idées galoisiennes (théorie de l'ambiguïté)* (12 mai 2007)
- *Dix regards sur la mathématique contemporaine* : chapitre V (Spartacus-idh, 2021)

François Nicolas

Exposés

- *D'une longue marche de la modernité musicale, à la lumière de l'algèbre galoisienne* (20 janvier 2018) [14]
- *Enquête mamuphique sur la théorie de Galois* (7 avril 2018) [15]
- *De la solidarité de groupe dans la théorie galoisienne* (13 octobre 2018) [16]

Polycopié

Polycopié mamuphi (2018), cent pages dont voici les grandes parties :

Intermède biographique : Évariste

0 – Travail sur des équations particulières
I - Trois structures algébriques
    - Anneau des polynômes
    - Corps de nombres
    - Groupes de symétrie
II - Correspondance de Galois
    - Notion-clef : invariance
    - Trois embrayages : $\mathcal{D}\mathbb{P}\rightleftarrows\Delta K$; $\mathcal{D}\mathbb{P}\rightleftarrows\nabla G$; $\Delta K\rightleftarrows\nabla G$
    - Logique
III - Théorie de Galois
IV - Raisonances intellectuelles

Prolongements de la théorie de Galois

---

[13] www.youtube.com/watch?v=BAmhQle-uvA&pbjreload=101
[14] www.entretemps.asso.fr/Nicolas/2018/Galois.htm
[15] notes d'exposé disponibles sur demande
[16] www.entretemps.asso.fr/Nicolas/2018/Galois-13-10-2018.html

- Généralisations (M-I)
- Abstractions (M-II)
- Extensions (M-III)

ANNEXES

- Annexe 0 : *Documentation commentée*
- Annexe 1 : *Polynômes*
- Annexe 2 : *Florilège d'équations quintiques*
- Annexe 3 : *Permutations*
- Annexe 4 : *Groupes*
- Annexe 5 : *Espaces vectoriels et algèbres*
- Annexe 6 : *Anneaux et idéaux*
- Annexe 7 : *Quotients*
- Annexe 8 : *Corps*
- Annexe 9 : *Variances, morphismes, extensions*
- Annexe 10 : *Trois théorèmes fondamentaux (arithmétique, algèbre, analyse)*
- Annexe 11 : *Calculs effectifs de groupes de Galois*
- Annexe 12 : *Versions fonctionnelle/fonctorielle de la théorie de Galois*

***

(pour plus de détails mathématiques, voir le polycopié référencé dans la documentation précédente)

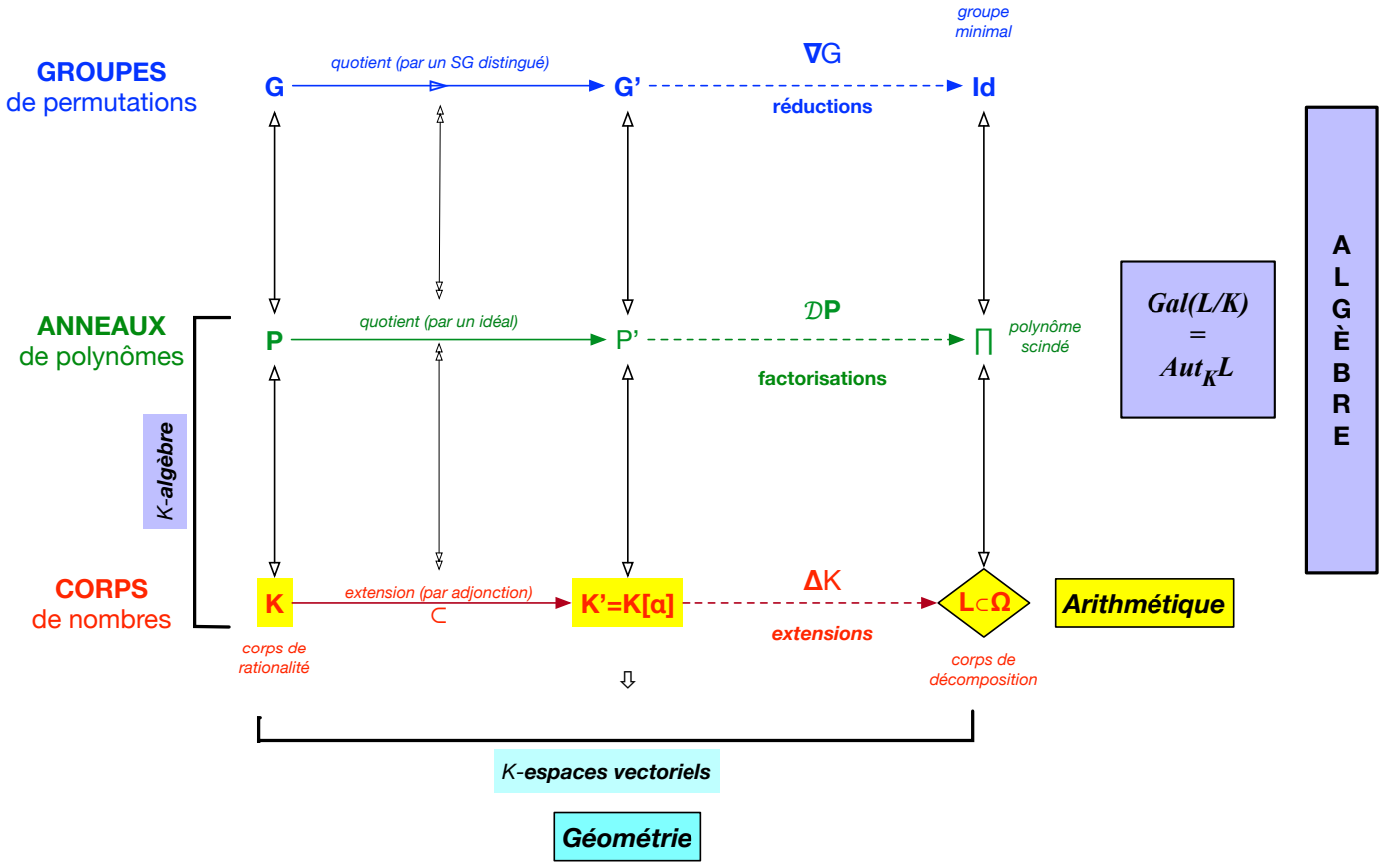
Logique générale du parcours

Pour démontrer constructivement (et non pas, comme Abel, par l'absurde) qu'une équation polynomiale d'ordre 5 – dite équation *quintique* - est en général irrésoluble par radicaux, on examine deux théorèmes :

1) Un théorème général : une équation polynomiale est résoluble si et seulement si son groupe de Galois est résoluble.
2) Un corollaire : l'équation quintique générale n'est pas résoluble car la résolution de son groupe de Galois bute sur un sous-groupe (dit *alterné*) irrésoluble.

I - Théorème général

L'algèbre des polynômes se divise dynamiquement de manière contravariante (c'est-à-dire selon deux ordres inverses) en une arithmétique des nombres et une géométrie des permutations (géométrie formalisée par groupes de Galois), dynamique que l'on peut diagrammatiser ainsi :



On explore cette dynamique selon les étapes suivantes.

1) D'un côté un polynôme peut être vu comme le « polynom » de ses racines : il « polynomme » un paquet de nombres algébriques ; on dira qu'il formalise algébriquement une propriété arithmétique.
   Ce faisant, l'algèbre des polynômes va permettre de contrôler une extension arithmétique de l'intérieur même du corps de définition (selon un quotientage de l'anneau des polynômes par des idéaux).
2) D'un autre côté, un polynôme configure également un groupe de permutations entre ses racines (dit groupe de Galois) ; on dira qu'il formalise algébriquement une propriété géométrique.
   Ce faisant, l'algèbre des polynômes va permettre d'associer la décomposition d'un polynôme donné à la réduction de son groupe de Galois.

3) Au total, la décomposition d'un polynôme va pouvoir se diviser en deux projections contravariantes :
   - une tour d'adjonctions-extensions du corps initial de rationalité K vers le corps ultime de décomposition L ;
   - un puits de sous-groupes du groupe de Galois initial G vers le groupe minimal *Id* terminal.

   Cette double décomposition, discrète (par étapes dénombrables, ou par « crans »), sera pas à pas *mesurée* (par la dimension des espaces vectoriels générés par l'interprétation des anneaux-quotients en adjonctions-extensions) et *bornée* (par la butée ultime de la réduction en sous-groupes sur le groupe minimal *Id* correspondant au parachèvement de la tour d'extensions dans le corps de L de décomposition).
4) On examine alors les trois conditions précises pour que « le pignon » polynomial « crante » correctement les deux « crémaillères » contravariantes : *extensions de corps* et *réductions de groupes* :
   - quotientages successives des anneaux de polynômes $\mathbb{Q}[X]$ par un *idéal* P[X] en sorte que le quotient $\mathbb{Q}[X]/P[X]$ ait une structure d'anneau [condition de crantage pour le pignon polynomial], et ce jusqu'à ce que la factorisation $\mathcal{D}P$ bute sur un polynôme (entièrement) scindé $\prod$;
   - extension *normale* K[α] des corps de résolution K en sorte qu'un polynôme irréductible y devienne séparable [condition de crantage pour la crémaillère arithmétique des corps], et ce jusqu'à ce que l'extension ΔK atteigne le corps de décomposition L propre au polynôme en question P ;
   - quotientage des groupes de permutations G par un sous-groupe *distingué* H en sorte que le quotient obtenu G/H ait bien une structure de groupe [condition de crantage pour la crémaillère algébrique des groupes], et ce jusqu'à ce que la réduction de groupe ∇G atteigne le groupe minimal *Id*.
5) On mesure, pas par pas, la coordination de ces trois dynamiques (sur les anneaux de polynômes, les corps de nombres et les groupes de permutation) par la progression de la dimension des K-espaces vectoriels associés.

La dynamique de décomposition des polynômes

Voir l'annexe 6 du polycopié

C'est par exemple celle-ci :

$$x^5-3x^4-x^3+3x^2-2x+6$$
$$= (x-3)(x^2-2)(x^2+1)$$
$$= (x-3)(x-\sqrt{2})(x+\sqrt{2})(x^2+1)$$
$$= (x-3)(x-\sqrt{2})(x+\sqrt{2})(x-i)(x+i)$$

Anneau-quotient

Plus techniquement, la chose prend la forme suivante :

Soit un polynôme P(x) sur l'anneau des polynômes $\mathbb{Q}[X]$ ou $\mathbb{R}[X]$ ou $\mathbb{C}[X]$. On peut lui associer l'idéal [17] des polynômes multiples de P(x) c'est-à-dire tels que P(x) les divisent. L'anneau quotient $\mathbb{Q}[X]/P(x)$ sera structuré par la relation d'équivalence entre polynômes : $Q(x) \equiv Q'(x)_{\text{mod } P(x)}$ si Q/P et Q'/P' ont même reste R (Q=PS+R et Q'=PS'+R).

D'où le lien entre quotientage de polynômes (cf. leur décomposition) et structures d'anneau-quotient…

La dynamique extensive des corps

Voir l'annexe 9 du polycopié

[17] Ici, la propriété des idéaux qui nous intéresse est la possibilité de travailler *modulo* cet idéal car le quotient d'un anneau par un idéal (sous-groupe additif, stable par multiplication) est lui-même un anneau, l'anneau-quotient.

Corps

Un corps est un monde fermé sur lui-même par deux opérations sur ses objets : l'addition et la multiplication.
C'est ce caractère fermé sur soi qui nous intéresse ici, en particulier pour l'opération d'extension par adjonction : par exemple, quand on adjoint $\sqrt{2}$ à $\mathbb{Q}$, il faut s'assurer que $\mathbb{Q}[\sqrt{2}]=\{p+q\sqrt{2}\}$ est bien fermé sur lui-même, constitue donc un nouveau corps dont $\mathbb{Q}$ est une partie, un sous-corps :

$$\mathbb{Q}=\{p\} \subset \mathbb{Q}[\sqrt{2}]=\{p+q\sqrt{2}\}$$

Par exemple on vérifie facilement que

- $(p+q\sqrt{2})+(p'+q'\sqrt{2})=(p+p')+(q+q')\sqrt{2}$ qui appartient bien à $\mathbb{Q}[\sqrt{2}]$
- $(p+q\sqrt{2}).(p'+q'\sqrt{2})=(p.p'+2q.q')+(p.q'+p'.q)$ qui appartient bien à $\mathbb{Q}[\sqrt{2}]$

et donc que l'addition et la multiplication sont internes au corps étendu $\mathbb{Q}[\sqrt{2}]$.

Série d'extensions de corps

On va donc travailler sur une série d'extensions de corps où chaque corps devient sous-corps du corps étendu suivant. Le but est d'atteindre ainsi le corps minimum L (plus restreint que $\mathbb{A}$, $\mathbb{R}$ ou $\mathbb{C}$) sur lequel le polynôme de départ sera entièrement décomposable, c'est-à-dire *scindé*.

Pour le détail technique, voir plus loin.

La dynamique réductrice des groupes

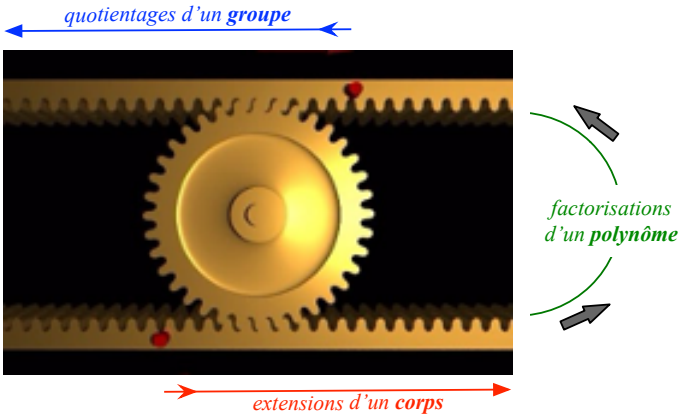
Voir l'annexe 4 du polycopié

Inversement (de manière « contravariante »), on va travailler sur une série de réductions de groupes.

Pour le détail technique, voir plus loin

Le crantage

Pour articuler ces trois dynamiques, prenons l'image d'une crémaillère, mise en œuvre par la dynamique (décomposante) des polynômes et agissant par crans successifs, d'un côté sur la dynamique (extensive) des corps et d'un autre côté, en sens inverse, sur la dynamique (réductrice) des groupes.



[Arithmétique de nombres]

Extensions L:K

Une extension (de corps) est un monomorphisme $K \rightarrow L$ (où $K \subset L$). On la note L:K

Exemples : $\mathbb{R}$:$\mathbb{Q}$, $\mathbb{C}$:$\mathbb{R}$, $\mathbb{Q}[\sqrt{2}]$:$\mathbb{Q}$…

K-espace vectoriel

Soit l'extension L:K. On définit dans L une structure d'espace vectoriel sur K en faisant opérer les éléments de K comme scalaires sur les éléments de K.
L est K-espace vectoriel (e.v. sur K) de dimension [L:K]
Degré de l'extension L:K = [L:K]. Le degré [L:K] de l'extension L:K est la dimension de L considéré comme espace vectoriel sur K

Extension → Espace vectoriel dont la dimension → le degré de l'extension.

Loi de la tour

Si K, L, M sont des sous-corps de $\mathbb{C}$ et que $K \subseteq L \subseteq M$, alors : $[M:K]=[M:L][L:K]$. On multiplie donc les degrés des extensions emboitées ou successives.

Adjonctions

Adjonction de α à K $\Longrightarrow$ extension notée $K[\alpha]$
L'extension L:K est simple si $L=K[\alpha]$ pour quelque $\alpha \in L$.
Une extension finie est une extension dont le degré est fini. Toute extension finie peut être obtenue comme séquence d'extensions simples.
Une extension L:K est algébrique si tout élément de L est algébrique sur K.

Corps de rupture

Le corps de rupture de P sur K est l'extension L:K telle que $\exists x : P(x)=0$ avec $L=K[x]$

Corps de décomposition (*splitting* fields)

P se décompose sur K s'il peut être exprimé comme $k\prod(x-a_i)$
Le corps M est un corps de décomposition pour P sur K si $K \subseteq M$, si P se décompose sur M et si M est minimal pour ce faire (si $K \subseteq M' \subseteq M$ avec P se décomposant sur M', alors M'=M).

Normalité

Une extension L:K est normale si tout polynôme irréductible sur K qui a une racine sur L y a toutes ses racines.
Voir la propriété de solidarité entre racines : « si une, alors toutes ! ».

Clôtures normales

Une clôture normale de L:K est la plus petite extension N:L avec N:K normale.

[Algèbre de groupes]

Groupes

De manière informelle, un groupe est un ensemble construit autour d'une relation qui soude les éléments deux à deux et les équilibre-symétrise autour d'un point d'équilibre (élément neutre).
Un groupe est donné par une loi de composition interne sur un ensemble c'est-à-dire une opération qui, à deux éléments quelconques, associe un élément (avec élément neutre, symétrie et associativité).

- La première définition abstraite du groupe sera donnée après Galois par Arthur Cayley (1821-1895).
- La formalisation définitive de la théorie de Galois sera donnée par Emil Artin (1898-1962).

L'ordre d'un groupe est sa cardinalité (nombre de ses éléments).

Didactiquement…

1) L'opération * maintient dans G.
2) Peu importe l'ordre du parenthésage (associativité)
3) Il y a un élément sans effet (élément neutre).
4) On peut faire marche arrière (élément inverse).

Réduction de groupes

Réduction

Deux analogies :

- décomposition d'un nombre entier positif en nombres premiers ;
- décomposition d'un polynômes en monômes $(x-\rho_j)$.

Il s'agit ici de construire une suite finie décroissante de sous-groupes G_i (distingués : G_{i-1} est distin-

gué dans G_i avec G_i/G_{i-1} commutatif) et s'achevant à Id={1} :

$$G_n \supset G_{n-1} \supset \ldots \supset G_1 \supset G_0 = Id = \{e\}$$

Pour ce faire, les étapes sont :

- notion de sous-groupe d'un groupe donné ;
- notion de groupe-quotient ;
- notion de sous-groupe distingué (ou *normal* ou *invariant*) ;
- $\Longrightarrow$ un groupe est simple ou résoluble.

Sous-groupe

Une partie des permutations qui forment à elles seules un groupe.

Ex. les permutations de $\pm\sqrt{2}$ dans $(x-2)(x^2-2)(x^2+2)=0$

Groupe-quotient

Si H est sous-groupe de G, soit g un élément fixe de G (une permutation) et h un élément variable de H. Soit gh la permutation composée et soient gH l'ensemble de ces permutations composées. Les gH partitionnent G : on note G/H cette partition.

Si G est fini, Card (G/H)= Card(G)/Card(H)

Le but est alors d'assurer que G/H aura une structure de groupe.

Pour cela, la condition sur H va être que H soit un sous-groupe distingué dans G.

Sous-groupe distingué

On parle aussi sous-groupe *normal* ou *invariant*.

Attention

- C'est une propriété relative car un groupe est distingué *dans un groupe donné* (dont il est sous-groupe).
- La relation « être distingué dans » notée $H \lhd G$ n'est pas transitive.

L'idée directrice est qu'un sous-groupe H distingué dans G, c'est-à-dire stable par conjugaison, va diviser G en un nouveau groupe quotient G/H

Définition : $H \subset G$ est distingué dans G si $\forall h \in H$ et $\forall g \in G$ alors $ghg^{-1} \in H$. Autrement dit, $\forall g \in G$ on a $gH=Hg$.

On note cela $H \lhd G$ ou $H \trianglelefteq G$.

Si G est abélien, tout sous-groupe y est distingué puisque, dans ce cas, $ghg^{-1} = g^{-1}gh = h$.

L'idée est la suivante.

G et h un élément variable de H) forment une partition de G notée G/H.

On veut maintenant mettre une structure de groupe sur G/H avec pour produit

$$gH.g'H := gg'H$$

Mais attention : ici, H intervient deux fois et peut donc intervenir avec deux éléments différents : d'abord avec h, puis avec h'. Il faut donc s'assurer, par une condition supplémentaire, que H ne va pas dépendre de l'écriture de tel ou tel élément h ou h'.

Pour que le produit précédent soit bien défini, il faut alors s'assurer que

$\forall g, g' \in G$ et $\forall h, h' \in H$ on a bien $ghg'h' \in gg'H$ c'est-à-dire que $hg' \in g'H$

Il faut pour cela que

$$\forall h \in H \text{ et } \forall g' \in G : (g')^{-1}hg' \in H.$$

Un sous-groupe *distingué* (ou *normal* ou *invariant*) sera alors un sous-groupe stable par conjugaison c'est-à-dire tel que si $\forall h \in H$ et $\forall g \in G$ alors $\boxed{\mathbf{ghg^{-1} \in H}}$. Autrement dit, $\forall g \in G$ on a $gH=Hg$.

Il est alors clair que tout sous-groupe commutatif est distingué car dans ce cas :

$$\forall g \; ghg^{-1} = gg^{-1}h = h \in H.$$

Groupes simples

Un groupe simple est un groupe non trivial n'ayant pas d'autres sous-groupes distingués que lui et que le sous-groupe trivial à un élément Id.

Interprétation : c'est un groupe non résoluble, l'équivalent en arithmétique d'un nombre premier.

C'est le contraire d'un groupe résoluble comme le nombre premier est en arithmétique le contraire d'un nombre décomposable.

Groupes résolubles

Définition : il existe une suite finie décroissante de sous-groupes G_i distingués (G_{i-1} distingué dans G_i avec G_i/G_{i-1} commutatif) et s'achevant à Id={1} :

$$G_n \supset G_{n-1} \supset \ldots \supset G_1 \supset G_0 = Id = \{e\}$$

Interprétation : on peut le décomposer comme on décompose certains polynômes en $\prod(x-\rho_j)$. C'est le pendant de la notion d'équation résoluble par radicaux.

Point important : tout groupe commutatif (ou abélien) est résoluble puisque tout sous-groupe y est distingué et génère donc, par quotientage, un sous-groupe.

II - Corollaire spécifique pour l'équation quintique

En général, une équation quintique n'est pas résoluble par radicaux car la décomposition de son groupe de Galois vient buter sur un sous-groupe distingué simple c'est-à-dire irrésoluble : le groupe alterné A_5 à 60 éléments.

La démonstration du caractère irrésoluble de A_5 est combinatoire, laborieuse et sans grand intérêt immédiat pour notre propos. On la trouve au demeurant facilement sur le web. [18]

Théorème de Galois : l'équation quintique générale configure une extension dont le GG a A_5 pour SG distingué. Or A_5 est un groupe simple c'est-à-dire irrésoluble. Donc, en général, le GG de l'équation quintique n'est pas résoluble.

(pour plus de détails, voir le polycopié et ses annexes)

Groupes alternés

Un groupe alterné [19] est un sous-groupe distingué du groupe symétrique S_n, constitué des permutations paires c'est-à-dire des permutations produites par un nombre pair de transpositions (échanges de deux éléments, les autres restant fixes).
Son ordre est n!/2

A_5

Groupe des rotations laissant invariant un icosaèdre (ou son dual, le dodécaèdre).
A_5 est le premier groupe de l'*Atlas des groupes finis simples*, car c'est le groupe fini simple dont l'ordre (60) est minimal.

***

[18] à commencer dans la page Wikipedia consacrée au *Groupe alterné* :
https://fr.wikipedia.org/wiki/Groupe_altern%C3%A9

[19] Les groupes alternés sont la structure sous-jacente de casse-têtes mathématiques comme le taquin ou le Rubik's Cube !

CORRECTIF : BREF RETOUR SUR LA LEÇON PRÉCÉDENTE (COUPURES DE DEDEKIND)

J'ai pataugé la fois dernière pour démontrer que tout rationnel se trouvait bien incorporé à la coupure-somme C=A+B.
Cela a tenu au fait que, le nez sur le tableau et toutes notes de cours oubliées, j'ai mal caractérisé la somme de deux coupures.
La bonne manière de procéder est celle-ci.

Soient deux coupures $A:=A_1|A_2$ et $B:=B_1|B_2$
La somme A+B=C sera la coupure $C_1|C_2=(A_1+B_1)|(A_2+B_2)$ ainsi définie :
Soit $q\in\mathbb{Q}$;

- si $\exists(a_1\in A_1$ et $b_1\in B_1)$ avec $a_1+b_1\geq q$, alors $q\in C_1$;
- sinon, $q\in C_2$.

Il va alors de soi que tout rationnel appartient bien à l'une des deux parties C_1 ou C_2 de la coupure-somme C=A+B.

La double erreur commise était

1) de poser que $q\in C_1$ si $\exists(a_1\in A_1$ et $b_1\in B_1)$ tels que $q=a_1+b_1$ (au lieu de $q\leq a_1+b_1$: « = » au lieu de « ≤ ») ;
2) de poser que $q\in C_2$ si $\exists(a_2\in A_2$ et $b_2\in B_2)$ tels que $q=a_2+b_2$ (au lieu de définir tout simplement C_2 comme partie complémentaire de C_1 dans $\mathbb{Q}$).

***