De la solidarité de groupe dans la théorie galoisienne

(séminaire *mamuphi*, Ircam, samedi 13 octobre 2018)

- François Nicolas -

Deux cents ans après Galois, Alain Connes déclare qu'il lui a fallu « *beaucoup de temps* » et « *énormément de travail* » en 2011 pour arriver à « *comprendre la pénétration de la pensée de Galois* » et prendre conscience de ce que « *sa pensée garde son potentiel de mise en mouvement* » et cette « *fulgurance qui montre la voie à suivre* ». [1]
Pour mieux rétablir l'idée galoisienne d'*ambiguïté*, Connes délaisse provisoirement les structures algébriques abstraites que la modernité bourbakiste a retenues (*groupes* de symétrie des k-automorphismes, *anneaux* des polynômes, *corps* de résolution, *espaces vectoriels* et *k-algèbres* des extensions…) pour réactiver l'étonnement premier : il existe des relations *rationnelles* entre racines *non rationnelles* d'une même équation polynomiale, et c'est l'étude systématique de ces relations qui fonde la théorisation galoisienne avant qu'elle ne devienne officiellement « la théorie de Galois ».
Ce retournement rétablit une continuité Lagrange-Galois (sous le signe des « résolvantes » auxiliaires) pour mieux mettre en évidence le pas gagné par Galois : la lettre x ne symbolise plus tant une inconnue individuée que le membre générique d'un collectif solidaire, l'enjeu de l'équation n'est plus tant sa résolution (en x) que la caractérisation de son groupe si bien que les structures algébriques (dégagées dans la seconde vague de la modernité algébrique par Steinitz, Artin…) se réassurent ainsi dans leur capacité à formaliser le modèle polynomial.

Ce réancrage de la théorie dans son modèle constituant invite à repenser ce que *modernité* (ici algébrique) veut dire : par-delà le risque de l'abstraction formaliste où la syntaxe cultive ses capacités autoréférentielles (le « modernisme »), le retour à la sémantique originelle revivifie le travail théorique en autorisant quelques nouvelles interprétations de la formalisation patiemment élaborée et, par-là, quelques nouvelles extensions théoriques (songeons à la notion contemporaine de *perfectoïde* [2] venant explorer les parentés formelles d'espace géométrique entre l'algèbre polynomiale et l'arithmétique p-adique).
Ce faisant, le travail théorique avoue le secret commun à ses différents modèles en le formalisant : ainsi la forme du secret polynomial va se donner en l'idée de groupe qui formalise la solidarité secrète des racines (« l'ambiguïté » syntaxique avoue la solidarité sémantique des racines « conjuguées », donc gémellaires).
Ce qui caractériserait alors le travail théorique moderne serait que les secrets des modèles ne relèveraient plus d'une dissimulation (voir la logique infantile de l'objet caché pour mieux préparer la surprise de sa réapparition) qu'une mise au jour suffirait alors à dissiper, mais d'une singularité (dont Hironaka délivre le chiffre : une configuration locale qui avoue, par quelque irrégularité phénoménale, que deux tendances globalement orthogonales – c'est le secret d'ensemble - y sont rendues indiscernables). Dans notre cas, la théorie algébrique ne vise plus, comme dans l'algèbre classique, la résorption « par radicaux » du secret polynomial (tout classicisme ne répand-il pas quelque parfum d'enfance ?) mais l'aveu de sa singularité sous forme d'un groupe de solidarité entre racines.

Au total, on aurait donc la périodisation suivante :
- La première vague de la modernité algébrique (XIX°) avoue l'existence singulière d'un *groupe* qui reste pratiquement incalculable – d'où l'incompréhension tenace des « réalistes ».
- La seconde vague (première moitié du XX°) autonomise la forme de cet aveu, la séparant de la singularité secrète du polynome, par l'étude des nouvelles structures algébriques ainsi dégagées (d'où le risque « moderniste » d'un certain péril formaliste).
- La troisième vague (à partir des années 60), celle-là même qu'il s'agit cinquante ans plus tard de ressaisir inventivement (voir les chantiers en cours autour de Grothendieck) contre les sirènes démobilisatrices du consentement postmoderne, réancre la forme générale de l'aveu dans les secrets algébriques spécifiques en assumant consciemment qu'*un secret avoué reste un secret* (Lacan) : ainsi Connes, retournant à la théorie galoisienne d'avant « la théorie de Galois », éprouve que l'aveu, loin de dissiper

[1] *Sur Évariste Galois* (revue *Secousse*, n°6, mars 2012) : http://www.revue-secousse.fr/Secousse-06/Carte-blanche/SkS06-Connes-Galois.pdf
[2] Voir Peter Scholze (Médaille Fields 2018) : https://www.pourlascience.fr/sd/mathematiques/medaille-fields-peter-scholze-loracle-de-larithmetique-14428.php.
Sur les perfectoïdes : http://smf4.emath.fr/Publications/Gazette/2017/154/smf_gazette_154_60-64.pdf et https://www.youtube.com/watch?v=UfjaResU3tI

le secret, le réactive en amplifiant ses échos.

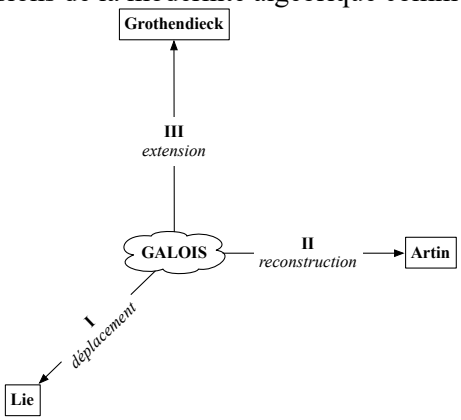
Ce retour contemporain à la théorie galoisienne s'avère gros de r*ai*sonances pour les modernités musicale (composer en « groupant » des voix ?), mamuphique (« grouper » mathématiques, musique et philosophie ?) et politique (« justice » comme nom du groupe – infini - *Humanité* ?).

« *La longue marche à travers la théorie de Galois* » Alexandre Grothendieck

« *La théorie de Galois est devenue tellement classique en mathématiques que les textes qui la présentent sont pour la plupart d'une facilité apparente qui est déconcertante et terriblement trompeuse car, en trivialisant les énoncés, elle en masque souvent la portée métamathématique. Il n'est donc sans doute pas inutile, même pour le mathématicien professionnel, de relire ces textes avec la fraicheur nécessaire,* i.e. *en essayant de réfléchir directement aux énoncés sans utiliser l'artillerie lourde.* » Alain Connes [3]

À l'initiative d'Alain Connes, il s'agit de reprendre Galois et sa théorie des groupes par-delà la « Galois Theory » [GT] formalisée par Emil Artin (années 30-40) et Bourbaki, avant même son déplacement par Lie (⟹ groupes de Lie), donc en son temps 0.

Cf. trois moments-dimensions de la modernité algébrique comme de toute modernité [4]:



Il s'agit d'exposer la théorie galoisienne (≠ de GT) en mettant à plat ses étonnements, ses questions et ses enjeux premiers, tels qu'ils peuvent se constituer avant même que n'existent les groupes, les anneaux, les corps, les espaces vectoriels et les k-algèbres, donc avant Dedekind.

Cf. ontogenèse : méthode d'exposition qui rapproche le Galois inventant la modernité algébrique et par là la modernité mathématique (le deuxième sera Riemann : les groupes de Galois et les surfaces de Riemann composent le premier temps de la modernité mathématique [5]) d'un mathématicien naïf, disons un lycéen issu de Terminale.

[3] 2011 : « La pensée d'Évariste Galois et le formalisme moderne ». http://www.alainconnes.org/docs/galoistext.pdf
[4] Pour les révolutions R.E.D., voir *Hétérophonies/68* : https://heterophonies68.wordpress.com/
[5] On y reviendra avec l'examen du travail de Zalamea…

I. La situation polynomiale et ses problèmes

Didactique non bourbakiste (cf. Stewart) : commencer par degré 5 puis généraliser à n (cf. « soit maintenant 5=n ») plutôt que l'inverse (« soit maintenant n=5 »).

∏⟹∑ !!!

∏

Posons le problème en exposant les polynômes à partir de leur forme $P(x)=\prod(x-r_j)$

Expressions

Assemblons un collectif de manière extensionnelle par construction élémentaire progressive d'expressions où x est un nombre indéterminé :

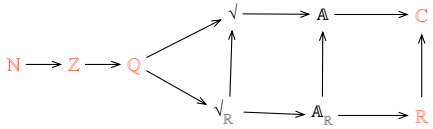
Expression polynomiale ∏	**R={r_j}**
(x-1)	{1}
(x-1)(x-2)	{1, 2}
(x-1)(x-2)(x-3)	{1, 2, 3}
(x-1)(x-2)(x-3)(x-4)	{1, 2, 3, 4}
(x-1)(x-2)(x-3)(x-4)(x-5)	{1, 2, 3, 4, 5}
(x-3)(x-√2)(x-π)	{3, √2, π}

Fonctions

Ces expressions polynomiales donnent lieu à des fonctions P(x) où x est un nombre variable :

par ex. P(x)=(x-1)(x-2)(x-3)(x-4)(x-5)

Un nombre peut appartenir à N, Z, Q, R ou C – ici le nombre variable x appartient à un corps, et les corps commencent avec Q.



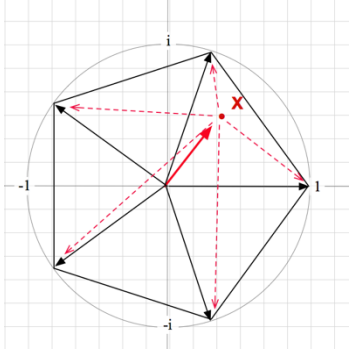
Qu'est-ce que « mesure » cette fonction P(x) ? Elle mesure l'écart synthétique de x à la « base » {1, 2, 3, 4, 5}. Cette « base » constitue les « racines » de la fonction polynomiale : R={r_j}

Exemple

$$f(x)=x^5-1$$

$$x^5-1=(x-1)(x-e^{2i\pi/5})(x-e^{4i\pi/5})(x-e^{6i\pi/5})(x-e^{8i\pi/5})=(x-1)(\mathbf{x^4+x^3+x^2+x+1})$$

La fonction $f(x)=x^5-1=\prod(x-e^{\frac{k.2i\pi}{5}})$ mesure l'écart cumulé de x à chaque racine :



Ces racines - les x qui assurent que $P_n(x)$ vaut 0 – constituent bien la base de la fonction.

Voir ici la différence entre $P(x)=x^5-1$ et $P'(x)=(x-1)^5$ ou entre $[x^5-1=0]$ et $[(x-1)^5=0]$.

La première équation a cinq racines différentes : $x=\sqrt[5]{1}=\{e^{\frac{k.2i\pi}{5}}\}$; la seconde a une racine quintuple (cinq fois la même racine 1).

$x^5=1$ formule qu'un rapport quintuple de x à soi-même vaut 1 quand $(x-1)^5=0$ formule que cinq fois, le rapport de x à 1 s'annule. D'un côté, cinq nombres ont le même rapport triple à soi ; de l'autre, un même nombre est quintuplé.

Équations

Cette fonction engendre un ensemble infini d'équations {P(x)=q} dans laquelle se distingue l'équation polynomiale canonique P(x)=0.
Pourquoi ? Car cette équation canonique détermine nos racines, donc ce que j'ai appelé « la base » de la fonction polynomiale sous sa forme ∏ ; on va le voir quand on va développer ∏ en ∑ :

$$x5-15x4+85x3-225x2+274x-120=0 \Leftrightarrow (x-1)(x-2)(x-3)(x-4)(x-5)=0$$

[voir plus loin p.15-16]

Au total, on a donc à faire à trois types différents de formalisations algébriques :

	la forme polynomiale est une	x est un nombre
$\prod(x-r_j)$	*expression*	*indéterminé*
$P(x)=\prod(x-r_j)$	*fonction*	*variable*
P(x)=q (de préférence 0)	*équation*	*inconnu*

∑

Comme l'on sait ∏⟹∑ :

$\prod(x-r_j)$	$R=\{r_j\}$	$\sum c_i x_i$
(x-1)	{1}	x-1
(x-1)(x-2)	{1, 2}	x^2-3x+2
(x-1)(x-2)(x-3)	{1, 2, 3}	$x^3-6x^2+11x-6$
(x-1)(x-2)(x-3)(x-4)	{1, 2, 3, 4}	$x^4-10x^3+35x^2-50x+24$
(x-1)(x-2)(x-3)(x-4)(x-5)	{1, 2, 3, 4, 5}	$x^5-15x^4+85x^3-225x^2+274x-120$
(x-3)(x-√2)(x-π)	{3, √2, π}	$x^3-(3+\sqrt{2}+\pi)x^2+(3\sqrt{2}+3\pi+\pi\sqrt{2})x-3\pi\sqrt{2}$

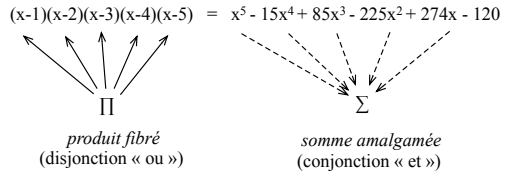
∏	la forme polynomiale est une	x est un nombre	∑
$\prod(x-r_j)$	*expression*	*indéterminé*	$\sum c_i x^i$
$P(x)=\prod(x-r_j)$	*fonction*	*variable*	$P(x)=\sum c_i x^i$
P(x)=q (0 de préférence)	*équation*	*inconnu*	**P(x)**=q (0 de préférence)

Notre polynôme P(x) a donc deux formes duales ∏/∑.

Noter que notre transformation $(x-1)(x-2)(x-3)(x-4)(x-5)=x^5-15x^4+85x^3-225x^2+274x-120$ procède d'un calcul (algébrique) à la lettre et donc « aveugle » (cf. René Guitart).
C'est la même lettre x des deux côtés, qui des deux côtés intervient 5 fois mais de manières bien différentes. Il faut s'arrêter un peu longuement sur cette différence, pour en restituer l'étonnement premier [6] car tout ceci est au principe même de notre problème : celui de la résolution par radicaux des équations polynomiales présentées initialement sous leur forme $\sum c_i x_i=0$.

Examinons les 2 équations (polynomiales) définies par ces 2 expressions (polynomiales) :

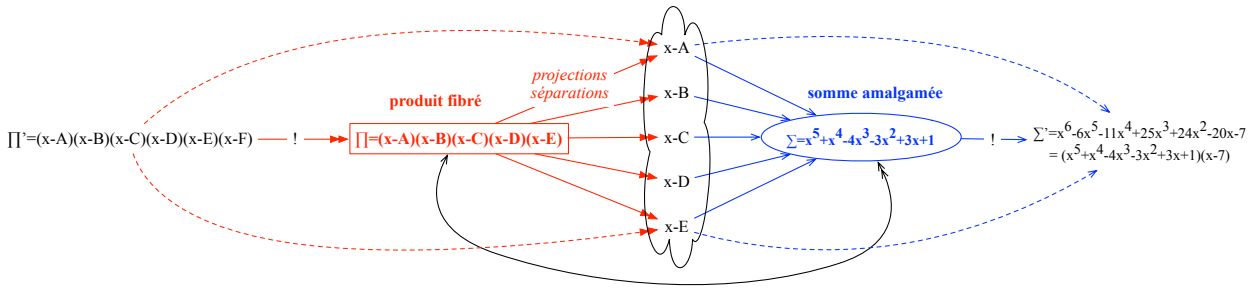
$$\prod(x-r_j)=0 \qquad\qquad \sum c_i x^i=0$$



x doit vérifier le 1° **ou** le 2° **ou**… le n° terme	x doit vérifier à la fois le 1° **et** le 2° **et**… le n° monômes

[6] celui qui m'a saisi quand pour la première fois l'enfant que j'étais à été confronté au secret de la lettre x

– ∏(x)=0 formalise R={r_j} extensionnellement selon une logique de produit fibré (*pullback* [7]) : multiplication de n monômes de degré 1 ;
– ∑(x)=0 formalise R={r_j} intensionnellement selon une logique de somme amalgamée (*pushout* [8]) : addition de n monômes de degré variable.



∑ formalise intensionnellement car il formalise les racines selon une propriété commune, vérifiée par chacune : on a bien $\sum(r_j)=\sum c_i r_j^i=0$
Comment comprendre cette propriété ?

Cf. logique sémantique de cette didactique : la syntaxe (et en particulier le calcul qu'elle autorise [9]) est tendanciellement « aveugle » et il nous faut une sémantique pour en comprendre la logique rationnelle.

Cf. danger du « formalisme » (propre à M-II) quand l'autonomie *relative* de la syntaxe ou de la théorie tend à s'absolutiser en se coupant de toute sémantique (en oubliant, en « refoulant » ses modèles) :

« formalisme » = refoulement du modèle et de l'interprétation sémantique

∑ formalise un rapport complexe (d'ordre n) et amalgamé (par somme) de la variable x à elle-même.
∑ formalise le rapport à soi que partagent toutes les racines.
∑ formalise la propriété *réflexive* qui fait équivaloir toutes les racines entre elles.

Ainsi le nombre 1 vérifie aussi bien les 5 propriétés suivantes qu'une infinité d'autres du même type :

- x-1=0
- x^2-3x+2=0
- x^3-6x^2+11x-6=0
- x^4-10x^3+35x^2-50x+24=0
- x^5-15x^4+85x^3-225x^2+274x-120=0

et s'il vérifie, par exemple la quatrième, c'est en tant que cette propriété est bien la seule qu'il ait en partage avec les trois autres nombres 2, 3 et 4.

Donc ∑ convertit la propriété 1∈{1, 2, 3, 4} en une propriété purement réflexive de 1 ne faisant pas intervenir explicitement les nombres 2, 3 et 4.
Cette conversion va évidemment être au principe de notre problème principal : comment dégager les racines d'un ∑ arbitrairement donné, comment passer d'une relation polynomiale réflexive ∑ à une relation polynomiale extensive ∏ ?

σ

La transformation ∏→∑ nous dote immédiatement d'une relation entre racines r_j explicites de ∏ et coefficients c_i explicites de ∑.

Prenons un exemple simple : (x-a)(x-b)(x-c)=x^3-(a+b+c)x^2+(ab+bc+ca)x-abc=x^3+c_2x^2+c_1x+c_0
On a :

1. c_3=1 [10]
2. c_2=a+b+c

[7] « *tiré en arrière* »
[8] « *poussé en avant* »
[9] Je rappelle : le niveau syntaxique correspond ici au niveau de la théorie dans la théorie des modèles, et c'est lui qui autorise des déductions et des calculs que le caractère purement « expérimental » du modèle (niveau sémantique) n'autorise pas.
[10] On va y revenir : on travaille ici systématiquement sur des polynômes unitaires (c_n=1), séparables (racines toutes différentes) à coefficients entiers. On démontre qu'on peut systématiquement ramener l'examen des polynômes rationnels (sur Q) à ce cas.

3. $c_1=ab+bc+ca$
4. $c_0=abc$

Formalisons cela en général : $c_i=\sigma_i(r_j)$ où σ_i désigne la somme systématique (et donc symétrique) de (n-i) produits de racines.

Ces relations $c_i=\sigma_i(r_j)$ sont les *sommes coefficients-racines*.
Notons que ces relations sont symétriques et rationnelles (elles sont triplement internes au corps Q : par les coefficients des sommes, par les puissances entières des produits intervenant dans ces sommes et par leurs résultats rationnels que sont les c_i) et symétriques. On peut les voir – et cela aura une grande importance dans la théorie galoisienne [11] – comme des relations rationnelles symétriques entre toutes les racines : on a ainsi par exemple ces deux relations rationnelles $\sum r_j=c_{n-1}$ et $\prod r_j=c_0$.

Notre espace de travail est donc ainsi constitué :

$$\prod \xrightarrow{\sigma_i(r_j)} \sum$$

∑⟹∏ ???

Posons-nous maintenant la question canonique : comment l'inverser ?

$$\prod \xleftarrow[c_i]{???} \sum$$

Pour cela, nous nous situerons désormais dans l'espace des polynômes

- unitaires (le coefficient c_n de x^n vaut 1),
- séparables (à racines simples : toutes les racines sont différentes),
- à coefficients entiers ($c_i\in\mathbb{Z}$).

On démontre facilement [12] qu'on peut se ramener à ce cas-là par opérations arithmétiques élémentaires sur les coefficients et par multiplication/division dans l'anneau des polynômes.

On part donc désormais d'une expression polynomiale $\sum c_i x^i$ avec $c_i\in\mathbb{Z}$.
On sait (théorème de Lagrange) qu'il y a n racines algébriques (donc sur $\mathbb{A}$ c'est-à-dire sur $\mathbb{A}_{\mathbb{C}}\neq\mathbb{A}_{\mathbb{R}}$) mais la forme $\sum$ de l'expression polynomiale ne la met pas au jour comme le faisait la forme duale $\prod$. Disons que, pour la forme $\sum$, ces racines sont secrètes et que la question posée est : comment travailler cette forme rationnelle (sur Q) peut avouer son secret c'est-à-dire mettre au jour ses n racines algébriques (sur A) ?

$$\sum \xrightarrow[c_i]{???} \prod$$

c_i sur $\mathbb{Q}$ $\qquad$ r_j sur $\mathbb{A}$

Rappel « sémantique » : l'expression $\sum$ amalgame un rapport complexe de x à lui-même qui formalise cet unique rapport à soi que toutes les racines partagent. En un sens $\sum$ ne nous dit rien d'autre que ce que $\prod$ nous dit aussi sous une autre forme : $\sum(x)=0 \leftrightarrow x\in R=\{rj\}$ mais il nous le dit « intensionnellement » (par une propriété discriminante de x) quand $\prod$ nous le dit « extensionnellement » donc explicitement (par la liste même des racines).
On peut voir $\sum$ comme filtrant l'ensembles des nombres algébriques pour ne sélectionner que les n nombres ayant la propriété réflexive $\sum$.
$\sum$ nomme rationnellement (dans Q) la propriété distinctive d'une racine quelconque, c'est-à-dire d'un élément quelconque du collectif R délimité par l'expression polynômiale.
Ainsi quand on écrit une équation polynômiale quelconque, on définit rationnellement une propriété réflexive d'un nombre inconnu qui, sans qu'on n'y voit goutte, délimite un strict collectif de n nombres algébriques tel que dire « x a la propriété en question » équivaut absolument à dire « x appartient à ce petit collectif ».

Amusons-nous un instant : le polynôme suivant [13]

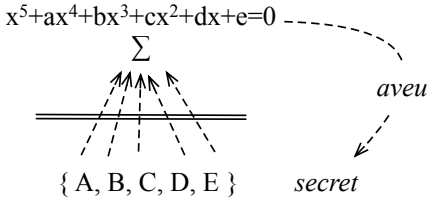
---

[11] qui va se construire sur l'examen systématique de l'espace fonctionnel constitué par toutes les fonctions rationnelles des racines…
[12] Voir par exemple Escoffier p. 222
[13] Pour information, j'utilise le petit logiciel en ligne, fort commode, https://www.mathway.com/fr/Algebra

$$x^5 - 9570x^4 + 36617600x^3 - 70023291150x^2 + 66921936063039x - 25571509333419600$$ [14]

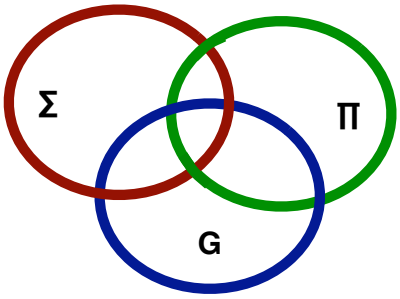
formalise que sa plus grande solution 2025 appartient au collectif {1789, 1871,1917, 1968}, autant dire qu'en 2025, une révolution d'importance mondiale pourrait survenir !

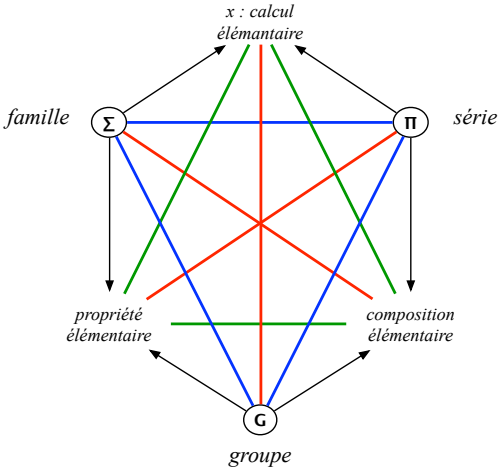
Notre secret peut être diagrammatisé ainsi :



Le point singulier est le suivant : en amalgamant le collectif des racines pour formaliser la propriété réflexive commune qui distingue chaque membre, ∑ le dissimule en le structurant, l'organise en le refoulant ! En effet ∑ transforme une liste amorphe d'éléments {A, B, C, D, E} en une famille délimitée (elle serait différent si on y ajoutait F ou si l'on en retranchait E) d'éléments partageant un trait distinctif commun qui les discrimine parmi l'infinité (dénombrable, rappelons-le) des nombres algébriques.
En un sens, ∑ avoue le secret de ∏ (le trait individuel qui solidarise cette famille à la différence de tout autre, le trait commun des éléments) tout en refoulant – par amalgame - la composition effective de cette famille.
À l'inverse, ∏ avoue le secret de ∑ (la composition élémentaire détaillée du collectif, la liste de ses membres) tout en refoulant - par simple listage - le trait commun à tous ses membres.
La résolution de ce double excès/manque va se faire par mise au jour de la manière dont les racines sont groupées, ce qui va rendre compte de leur solidarité collective, c'est-à-dire des relations directes entre membres du collectif (et non plus du trait familial partagé).

On pressent qu'on va avoir à faire ici au nœud borroméen de trois formalisations de la même solidarité : ∑/∏/G, autant dire à un hexagone logique [15] :





On a affaire à trois formalisations différentes et complémentaires du même collectif :

- ∑ formalise une *famille* caractérisée par un trait distinctif commun (sans que cette famille soit forcément solidaire).
- ∏ formalise une *collection* de membres juxtaposés, une série ou une file indienne (ni trait distinctif commun ni solidarité propre).
- G va formaliser un *groupe* rendu solidaire par les relations directes entre les membres.

G

Que veut dire « groupe » ? Que veut dire que plusieurs racines sont « groupées » ?

[14] =(x-1789)(x-1871)(x-1917)(x-1968)(x-2025)
[15] René Guitart a démontré que tout hexagone logique formalise le nœud borroméen de ses trois sommets contraires. Je conjecture ici la réciproque : tout nœud borroméen structure un hexagone logique à partir de ces sommets contraires.

Plus loin, on va distinguer systématiquement la manière dont les racines sont directement groupées par des relations rationnelles entre elles du Groupe de Galois [GG] proprement dit qui ne concerne qu'indirectement les racines : par leurs permutations (le GG est donc le groupe des permutations, non des racines). Mais pour le moment, gardons l'ambiguïté duale du Groupement.

Cela veut dire que dans Q, « rationnellement » donc, elles sont indistinguables, elles n'y sont pas nommables séparément ; dans Q, ces racines sont parfaitement gémellaires.

Ces racines sont cependant délimitées (définies sur $\mathbb{A}$, voire sur $\sqrt{}$) puisqu'il y a bien dans Q une nomination rationnelle de leur collectif solidaire : par un polynôme indécomposable sur Q du type (x^2-2) ou (x^2+1) ou $(x^5+x^4-4x^3-3x^2+3x+1)$.

Donc les permutations entre ces racines conjuguées sont indiscernables dans toute expression rationnelle - c'est-à-dire expression rationnellement construite à valeur rationnelle : expressions polynomiales définies sur Q à valeur dans Q (ainsi $\pm\sqrt{2}$ n'interviendra que dans des monômes d'exposant pair).

Point complémentaire (qui va avoir une importance dans la résolution par Galois du groupement) : la solidarité de groupe entre ces racines prend la forme d'une relation rationnelle directe entre ces racines - par exemple les deux racines conjuguées {A, B} de $(x^2-2)=0$ sont directement liées par la relation rationnelle directe : $A^2=B^2$ et les quatre {A, B, C, D} de $(x^4-2)=0$ sont directement reliées par la relation rationnelle $A^4=B^4=C^4=D^4$.

Au total, un groupe (qui peut être un sous-groupe) de racines se manifeste sous 4 traits :

- l'existence d'une nomination rationnelle de leur collectif comme tel (selon le trait distinctif que chaque membre partage) : voir le polynôme propre du groupe ;
- l'inexistence d'une nomination individuelle pour chacune (le polynôme n'est pas séparable dans Q) ;
- une indistinction rationnelle (« ambiguïté ») de leurs permutations (Q ne peut discerner une interversion des membres) ;
- une relation rationnelle directe entre elles (la solidarité qui constitue la gémellité entre racines se dit rationnellement).

Remarquons une différence importante entre les trois premiers traits et le quatrième : les trois premiers sont relatifs au corps Q puisqu'ils concernent la capacité de discerner rationnellement des nombres qui ne sont pas forcément rationnels. Par contre le quatrième trait désigne une relation absolue entre racines algébriques : $A^2=B^2$ ou $A^4=B^4=C^4=D^4$ vaut absolument quelle que soit la nature rationnelle ou non des racines quand $(x^2-2)=0$ ne peut nommer $\pm\sqrt{2}$ seulement sur Q.

Tout de même, comme on le verra, pour l'équation $x^5+x^4-4x^3-3x^2+3x+1=0$ dont les 5 racines réelles {A, B, C, D, E}={-1,9…, -1,3…, -0,2…, 0,8…, 1,6…}ne sont pas formulables par radicaux, on a $E=A^2-2$, $D=E^2-2$, $B=D^2-2$, $C+B^2-2$ et $A=C^2-2$.

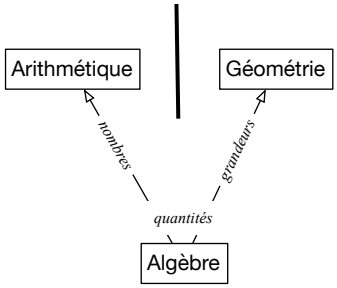
Le quatrième trait va être la porte d'entrée pour l'aveu galoisien du groupe secret.

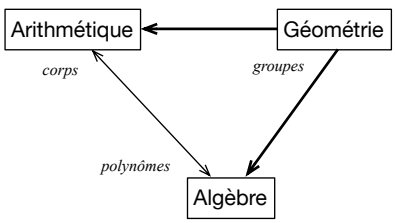
Pour le dire d'un mot, c'est ce trait qui concerne la dimension géométrique du groupement quand les trois autres concerne sa dimension arithmétique (liée au corps de résolution : de Q à C).

Algèbre-arithmétique-géométrie

Ce point a son importance : la théorie galoisienne reconfigure les rapports entre les trois grands domaines mathématiques : arithmétique, géométrie, algèbre.

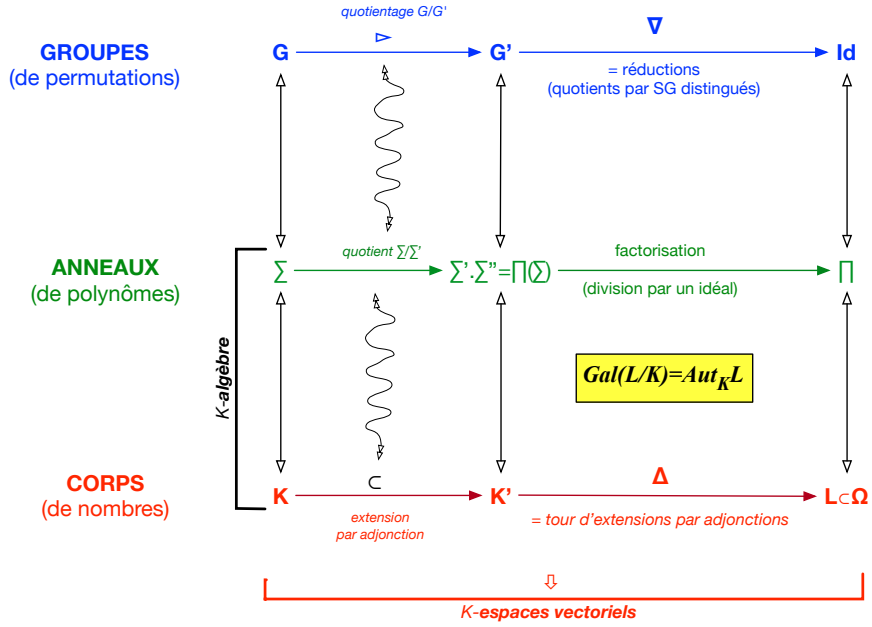
La naissance de l'algèbre avait constitué un pont entre les deux continents, dogmatiquement séparés par Aristote [16], de l'arithmétique non axiomatisée et de la géométrie euclidiennement axiomatisée en formalisant d'une unique manière par la lettre x des quantités aussi bien arithmétiques (nombres) que géométriques (grandeurs).





[16] Aristote prescrivait qu'on ne pouvait démontrer une proposition arithmétique en faisant intervenir des démonstrations géométriques (et vice versa).

La théorie galoisienne des groupes dispose cette fois la géométrie des groupes [17] en pont entre l'algèbre des polynômes et l'arithmétique des corps.
Voir ce schéma synthétique de la « Galois Theory » :



II. La théorie galoisienne

On peut comprendre la théorie galoisienne primitive, différente dont de la *Galois Theory* [*GT*], comme théorisation de la manière dont on peut passer de $\sum$ à $\prod$.

Fonctoriel/fonctionnel

L'idée va être de concevoir ce passage, dont on sait qu'il va donner dans la *GT* $\boxed{\frac{\nabla G}{\Delta K} = \frac{G \to Id}{\mathbb{Q} \to \mathbb{Q}[r_k]}}$ comme un espace fonctionnel : l'espace de fonctions polynomiales rationnelles car l'opérateur du travail Fonctoriel $\frac{\nabla G}{\Delta K}$ va être un travail sur les fonctions polynomiales à n variables généralisant en quelque sorte les $c_i=\sigma_i(r_j)$.
En effet, le point de départ de la *GT* est le groupe des substitutions (entre racines) indécelables dans Q par des polynômes rationnels, groupe qui concerne donc le rapport G/Q.
Posons que le rapport entre G et Q, qui va donner $\frac{\nabla G}{\Delta K}$, est un rapport Fonctoriel (entre deux catégories : celle des groupes et celle des corps) et que la manière de rapporter ces deux catégories est fonctionnel puisque ce sont des fonctions polynomiales $\mathbb{P}$ qui discriminent permutations décelables/indécelables : au point d'arrivée Id/Q[r_k], toutes les substitutions sont devenues décelables par $\mathbb{P}$ sur le corps étendu.
On voit donc que le fonctionnel constitue le Fonctoriel : $\mathbb{P}$ noue Fonctoriellement G et K ; ou : G est relié à K par $\mathbb{P}$.
On a

$$[\mathbb{P}]\frac{G}{K}$$

Remarquons, au passage, l'analogie avec notre point de départ :

$$[c_i = \sigma_i(r_j)]\frac{\sum}{\prod}$$

Les transformations internes à l'anneau P des polynômes relient fonctoriellement la catégorie des groupes et la catégorie des corps comme les sommes *coefficients-racines* corrèlent fonctionnellement la présentation duale d'un polynôme en somme de monômes ou en produit de polynômes simples.

Petite pause sur cette distinction

Le fonctionnel associe un élément et un seul à un ou plusieurs éléments.
Le fonctoriel est une correspondance entre structures. Il faut le comparer à une marche sur deux jambes : toute la correspondance de Galois est basée sur ce principe (avancer d'un côté – du côté des corps par AE – pour avancer ensuite de l'autre – du côté des groupes).

[17] La formalisation « naturelle » d'un GG est géométrique.

Mais le fonctoriel compte en fait 3 et pas 2 car il y a 1 correspondance entre 2 structures : la pensée fonctorielle avance sur deux jambes et il y a donc 1 pensée qui coordonne 2 jambes.
Dans notre situation, ce qui coordonne fonctoriellement la catégorie des groupes et celle des corps est l'anneau des plolynômes :

$$\frac{GROUPES\ (de\ permutations)}{CORPS\ (de\ définition)}\ ANNEAUX\ (des\ polynômes)$$

Groupements géométriques/algébriques

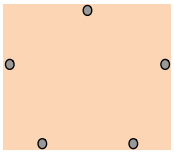
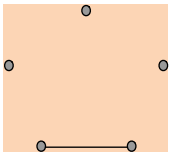
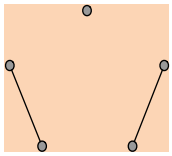
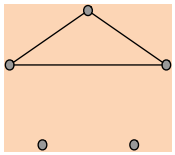
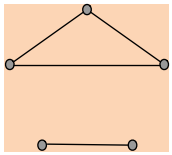
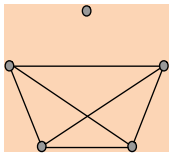
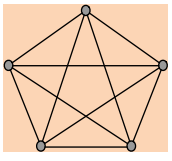
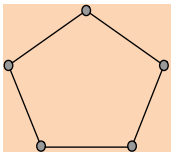
Il faut maintenant bien distinguer deux modes de groupements polynomiaux pour les racines :

- un mode de groupement direct entre les racines, qui ne fait pas intervenir leur corps de définition ; on parlera ici de groupement géométrique ;
- un groupe algébrique strict, le GG, dont les éléments ne sont pas les racines mais les permutations entre différents arrangements des n racines.

Détaillons.

Groupement géométrique

En détaillant quelques équations du 5° degré, on peut voir que les racines s'avèrent différemment regroupables, par exemple de ces 7 manières :

<table>
<tr><td colspan="2">$(x-1)(x-2)(x-3)(x-4)(x-5) \equiv \{1, 2, 3, 4, 5\}$
1+1+1+1+1
  </td></tr>
<tr><td>$(x-1)(x-2)(x-3)(x^2-2) \equiv \{1, 2, 3, \pm\sqrt{2}\}$
1+1+1+2
  </td><td>$(x-1)(x^2-2)(x^2+1) \equiv \{1, \pm\sqrt{2}, \pm i\}$
1+2+2
  </td></tr>
<tr><td>$(x-1)(x-2)(x^3-2)$
1+1+3
  </td><td>$(x^2-2)(x^3-2)$
2+3
  </td></tr>
<tr><td colspan="2">$(x-1)(x^4-2) \equiv \{1, \pm\sqrt[4]{2}, \pm i\sqrt[4]{2}\}$
1+4
  </td></tr>
<tr><td>$x^5-2=0$
5
  </td><td>$x^5+x^4-4x^3-3x^2+3x+1$
5
  </td></tr>
</table>

∑	∏	**R**	**G**
$x^5-15x^4+85x^3-225x^2+274x-120$	(x-1)(x-2)(x-3)(x-4)(x-5)	{1, 2, 3, 4, 5}	1+1+1+1+1 *=Id*
$x^5-6x^4+9x^3+6x^2-22x+12$	$(x-1)(x-2)(x-3)(x^2-2)$	$\{1, 2, 3, \pm\sqrt{2}\}$	1+1+1+2
	$(x-1)(x-2)(x^3-2)$		1+1+3
$x^5-x^4-x^3+x^2-2x+2$	$(x-1)(x^2-2)(x^2+1)$	$\{1, \pm\sqrt{2}, \pm i\}$	1+2+2
x^5-x^4-2x+2	$(x-1)(x^4-2)$	$\{1, \pm\sqrt[4]{2}, \pm i\sqrt[4]{2}\}$	1+4
	$(x^2-2)(x^3-2)$		2+3
	$x^5-2=0$		5
$x^5+x^4-4x^3-3x^2+3x+1$		{A, B, C, D, E} {-1,9…, -1,3…, -0,2…, 0,8…, 1,6…}	5

Ces relations directes entre racines ne sont pas dépendantes du corps de définitions : certes (x^2-2), indécomposable sur Q, peut se décomposer sur $\sqrt{}_{\mathbb{R}}$ en $(x+\sqrt{2})(x-\sqrt{2})$ mais la relation directe entre les deux racines $A^2=B^2$ c'est-à-dire ici $(\sqrt{2})^2=(-\sqrt{2})^2$ ne dépend pas du corps.
C'est elle que je diagrammatise par mes différents pentagones.

Groupe algébrique

Le groupe algébrique de Galois est, lui, relatif à une différence de corps puisqu'il concerne les substitutions de racines qui sont indécelables sur un corps donné et cette indécelabilité est relative à l'écart entre le corps de discernement des racines ($\sqrt{}_{\mathbb{R}}$ pour $\pm\sqrt{2}$ ou $\sqrt{}_{\mathbb{C}}$ pour $\pm i$) et le corps de définition des polynômes (ici Q) : sur Q, une permutation entre $\sqrt{2}$ et $-\sqrt{2}$ est indécelable par le polynôme (x^2-2) mais la même permutation ne l'est plus sur $\sqrt{}_{\mathbb{R}}$ ou A ou R ou C.

Résumons les différences :

groupement géométrique	**Groupe algébrique : GG**
racines	permutations
statique	dynamique
endogène ou direct	exogène ou indirect
« absolu » : $A^2=B^2$ $B=A^2-2$	relatif $(x^2-2) \mid (x+\sqrt{2})(x-\sqrt{2})$ $x^5+x^4-4x^3-3x^2+3x+1$ est indécomposable.

En un certain sens, le point de vue géométrique [18] est un en-deçà de l'algèbre de Galois, une sorte de transcendantal pour l'algèbre.
Cf. le point de vue moderne, lié à la révolution de la conception d'espace : non seulement les espaces non euclidiens et les surfaces de Riemann (prolifération des espaces par invalidation de l'unicité d'un espace naturel) mais, plus encore, les espaces fonctionnels/vectoriels/de Hilbert, etc. qui partagent alors avec l'espace einsteinien le fait que l'espace en question ne préexiste pas à ses objets car ces objets non pas peuplent l'espace en question mais le constituent : on passe en quelque sorte de « un espace et ses objets » à « des objets et leur espace propre ».
Cf. le rôle de la géométrie dans M-III : la géométrisation des mathématiques configure ce « tournant géométrique » que la mathématique oppose au « tournant logiciste et linguistique » de la philosophie analytique…

Nous allons donc parcourir la théorie des groupes selon deux parcours :
- un parcours fonctionnel partant de $\{P\}=\mathbb{P}$ pour voir comment il met en branle la correspondance fonctorielle $\frac{\nabla G}{\Delta K}$;
- un parcours fonctoriel partant de $\frac{\nabla G}{\Delta K}$ pour voir comment les différentes structures articulent fonctoriellement leurs transformations.

Dans le premier cas, le travail sur $\mathbb{P}$ se distribue en une dualité $\frac{\nabla G}{\Delta K}$ qu'il noue. Dans le second cas, le nouage de G et K (par les K-automorphismes du corps étendu L) engendre en $\mathbb{P}$ la résolution du polynôme de départ.

[18] Cf. remarque de Pierre Cartier sur mon exposé mamuphi de janvier 2018.

Comme on va le voir, le point de vue fonctionnel, remis en avant récemment par Alain Connes, majore la continuité Lagrange→Galois sous le signe des résolvantes ou fonctions auxiliaires. On dira que ce point de vue est néoclassique.
Le point de vue fonctoriel, lui, majore, le saut Galois/Lagrange sous le signe de la notion de groupe. On dira que ce point de vue est modernisant [19].

Point de vue fonctionnel

La présentation de ce point de vue, qui suit de près le texte originel de Galois, se trouve détaillée dans la brochure de l'APMEP. Elle est présentée en 2011 par Connes (voir 2011 à l'Acédémie) et par Bruno Poizat dans *In the Steps of Galois* (dir. Szczeciniarz…).

Résumons l'architecture en dix étapes :
1) construction d'une fonction auxiliaire V linéaire qui discrimine les n! arrangements ;
2) construction d'un polynôme $\wp$ de degré (n-1)! dont les racines sont toutes les valeurs de V pour tous les arrangements correspondants à une racine fixe r_α arbitrairement choisie ;
3) expression rationnelle de cette racine r_α ;
4) expression rationnelle des (n-1) autres racines ;
5) équivalence permutationnelle : choisir un autre point de départ donnerait engendrerait simplement une permutation des résultats ;
6) adjonction de racines entrainant l'incorporation d'autres racines ;
7) groupe de substitutions (GG) laissant inchangées toutes les fonctions rationnelles des racines ;
8) ce groupe est indépendant des choix arbitraires de départ (V et r_α) ;
9) analyse du calcul effectif de ce GG via la théorie des corps finis (de caractéristique non nulle) ;
10) algorithme à travers les différents corps finis dont l'ordre est un nombre premier (voir Frobenius et Cebotarev).

Détaillons seulement les premières.

Arrangements-permutations

Précisons d'abord : on appelle arrangement de n termes une mise en ordre donnée (une liste ordonnée).
Par exemple, quand n=5, nommons les 5 racines {A,B,C,D,E}.
Un arrangement est {A,B,C,D,E}. Un autre est {B,A,C,D,E}. Un troisième est {B,C,D,E,A}…
On appelle permutation l'opération de transformation d'un arrangement en un autre.
Par exemple, la substitution {B,A,C,D,E} $\Longrightarrow$ {B,C,D,E,A}.
Un arrangement est un état ordonné. Une substitution est une transformation entre états.

Ceci dit, on choisit usuellement un ordre de base, donc un arrangement canonique A_0 (dans notre cas {A,B,C,D,E}) et on présentera tout autre arrangement comme substitution à partir de cet arrangement A_0. On a donc une correspondance biunivoque entre arrangements et substitutions à partir de A_0 qui autorise de parler indifféremment des uns ou des autres.

1 - Fonction auxiliaire V

Examinons l'espace fonctionnel des fonctions polynomiales à n variables.

On connaît déjà les n *sommes coefficients-racines* : $\sigma_i(r_j)=c_i$
En particulier, les deux extrêmes $\sum r_j=c_{n-1}$ et $\prod r_j=c_0$.
Ces fonctions sont symétriques en leur n variables et ne prennent donc qu'une valeur quel que soit l'arrangement retenu.
Remarquons que cette propriété tient au fait que l'addition et la multiplication des nombres est commutative – les corps Q, R, C sont commutatifs.
Donc ici ABCDE=BACDE=BCDEA… et A+B+C+D+E=B+A+C+D+E+=B+C+D+E+A…

Cette propriété de commutativité aura une importance plus tard dans la réduction des groupes : il faudra qu'on divise un groupe par un sous-groupe distingué (c'est-à-dire aux racines solidaires) et que le groupe quotient soit commutatif (« abélien »).

[19] Nomination provisoire, faute de mieux…

L'idée de Galois est de choisir une fonction (linéaire) des n racines – « fonction auxiliaire » notée V - qui va être maximalement dissymétrique c'est-à-dire qui prend n! valeurs différentes pour les n! arrangements des racines.

Intuitivement, on voit qu'une telle fonction devrait pouvoir prendre la forme $\sum n^i r_i$ avec n entier.

Dans notre cas, par ex. $2A+4B+8C+16D+32E$ ou $10A+10^2B+10^3C+10^4D+10^5E$…

On pourrait aussi imaginer une fonction du type $\sum n_i r_i$ avec n_i entier ($n \in \mathbb{N}$).

Par exemple $A+2B+3C+4D+5E$ ou $3A+5B+7C+11D+13^E$ (nombres premiers)…

On démontre qu'une telle fonction existe toujours – un petit calcul combinatoire y suffit : il y a n^n nombres qui rapportent les racines entre elles (A/B, B/A, C/E, E/C…) soit un nombre fini. Il suffit donc de choisir pour coefficients de l'équation les nombres qui restent !

Remarque importante : Galois ne construit pas explicitement cette fonction V. Il démontre simplement qu'elle existe toujours.

Au passage, il démontre cela non par un raisonnement par l'absurde mais par le raisonnement constructif présenté ci-dessus. Simplement ce raisonnement constructif ne construit pas pour autant la fonction V : le principe de son existence est constructivement démontré mais pas son existence concrète.

On commence d'entrer ici dans la difficulté de la théorie : elle est principiellement constructive mais bien vite effectivement incalculable.

Faisons-le sentir par l'exemple suivant.

Nos polynômes de degré 5 sont les premiers à n'être pas, dans le cas général, résolubles par radicaux. Leur degré est fini et tout petit.

Il y a 5! arrangements différents de 5 nombres différents (soit 120) si bien que le nombre de substitutions qu'il y a entre ces 5!=120 arrangements est de 5!!=120!

Et c'est là que les choses plongent d'ores et déjà dans un gouffre car $120! \cong 10^{200}$, ce qui est un nombre rigoureusement impraticable [20].

D'où la double nécessité de

- démontrer des existences restant inaccessibles au calcul ;
- mettre en place des algorithmes qui vont calculer certaines de ces existences et étendre leur champ de calculabilité au gré des développements des puissances de calcul. Avec l'informatique, la puissance algorithmique a fait des bonds considérables mais, tout compté, on semble aujourd'hui en rester aux groupes d'ordre 10 [21].

Revenons à notre fonction auxiliaire V qui a pour caractéristique d'avoir n! valeurs différentes pour les n! arrangements de ses n variables.

Entre les deux extrêmes de nos fonctions sommes (une seule valeur) et de nos fonctions auxiliaires (n! valeurs), on a beaucoup de cas intermédiaires.

Par exemple :

- la fonction $\Delta=\prod(r_k-r_l)$ pour $k<l$ ne prend que deux valeurs $\pm\Delta$. C'est cette fonction qui est au principe du discriminant d'un polynôme : $\delta=\Delta^2$ (voir le fameux « b^2-4ac »)
- la fonction $F=r_1+0.r_j$ ou $F=ar_1^k+0.r_j$ (pour $j=2, \ldots, n$) prendra n valeurs (les n valeurs des n racines). C'est une fonction indicatrice d'une racine

[20] Pour information ce nombre de permutations entre arrangements d'un polynôme d'ordre 5 doit être rapproché du nombre d'atomes dans tout l'univers : 10^{80}.

[21] Voir la remarque d'Alain Connes (note 2 de sa conférence à l'Académie).

En résumé on a l'échelle suivante :

Nombre de valeurs différentes	Fonctions		Nombre de permutations stabilisatrices
1 totalement symétrique	$\sigma_i(r_j)=c_i$: $\sum r_j=c_{n-1}$ ou $\prod r_j=c_0$	sommes coefficients-racines	n!
2	$\Delta=\prod(r_k-r_l)$ $\Longrightarrow \pm\Delta \Longrightarrow \delta=\Delta^2$	discriminants	n!/2
n-1		Résolvante de Lagrange [22]	
n	$r_1+0.r_j$ ou $ar_1^k+0.r_j$	fonctions indicatrices des racines	(n-1)!
n! maximalement assymétrique	$\sum n^j r_j$ ou $\sum n_j r_j$ …	fonction auxiliaire de Galois, indicatrice des arrangements	1

2 - Polynôme $\wp$

À partir de la fonction auxiliaire V à n! variables (les n! arrangements des n racines), indicatrice des arrangements, on construit le polynôme $\wp$ de degré (n-1)! ainsi :
soit les (n-1)! arrangements $A(r_\alpha)_k$ commençant tous par la même racine fixe r_α arbitrairement choisie et soit les n(-1)! valeurs différentes de $V[A(r_\alpha)_k]=V(r_\alpha)_k$.
Composons le polynôme $\wp=\prod(r_\alpha)$ d'ordre (n-1)! ayant ces (n-1)! valeurs différentes de V pour racines : $\prod[Y-V(r_\alpha)_k]$.
Il est alors clair que pour $r_\beta=r_\alpha$, les $\prod(r_\alpha)$ et $\prod(r_\beta)$ n'auront pas de racines communes (puisque, par construction, la fonction V discrimine tous les arrangements possibles).
Donc r_α est la seule racine r_j à annuler le polynôme $\wp=\prod[R-V(r_\alpha)_k]$.
Il faut ici penser l'équation polynomiale $\wp$ réécrite comme polynôme en Y c'est-à-dire sous la forme $\sum c(r_\alpha)_i Y^i$ où les coefficients $c(r_\alpha)_i$ sont des combinaisons des $V(r_\alpha)_k$.

r_α est alors la seule racine du système d'équations :

- $P(r_j)=0$ (car r_α est racine du polynôme de départ)
- $\wp=\sum c(r_\alpha)_i Y^i=0$ (car tous les $V[A(r_\alpha)_k]=V(r_\alpha)_k$ sont, par construction, racines de $\wp$).

3 - Expression rationnelle de r_α

De ce système d'équations, on peut alors déduire r_α en fonction de $\mathcal{V}$=V(arrangement canonique de base), « par élimination euclidienne »[23] - ce point est délicat ; je passe…
On a donc $r_\alpha = f(\mathcal{V})$.

4 - Expressions rationnelles des (n-1) autres racines

On a de même une expression rationnelle des autres racines en fonction de $\mathcal{V}$: $r_j=f_j(\mathcal{V})$

5 – Équivalence permutationnelle

On démontre ensuite que remplacer $\mathcal{V}$ par une autre racine de $\wp$ donnerait une permutation des racines r_j. Donc choisir un autre point de départ donnerait engendrerait simplement une permutation des résultats.

À partir d'ici, je « saute à pieds joints » sur les détails plutôt obscurs – on comprend au passage l'intérêt d'enseigner aujourd'hui la *Galois Theory* plutôt que la théorie galoisienne telle qu'elle s'élabore dans les manuscrits d'Évariste.

Les étapes suivantes sont :

- l'adjonction de racines entrainant l'incorporation d'autres racines ;
- le groupe de substitutions (GG) laissant inchangées toutes les fonctions rationnelles des racines ;
- l'indépendance de ce groupe par rapport aux choix arbitraires de départ (V et r_α) ;

[22] Cf. pour les équations quadratiques : f(AB+CD, AC+BD, AD+BC) pour n=4
[23] Connes, p. 4

- l'analyse du calcul effectif de ce GG via la théorie des corps finis (de caractéristique non nulle) ;
- la construction d'une procédure algorithmique à travers les différents corps finis dont l'ordre est un nombre premier (voir Frobenius et Cebotarev) permettant la calculabilité effective de GG (pour n<10).

Laissons-là ce que j'ai appelé le point de vue fonctionnel centré sur les opérateurs fonctionnels aptes à discerner les structures algébriques à l'œuvre dans notre domaine de travail.
Le point de vue que j'appelle fonctoriel procède autrement : il s'intéresse au jeu des structures algébriques et ne prend en compte le travail fonctionnel que pour autant qu'il opère comme « le doigt qui montre la lune » : non pas en soi mais pour palper et tâter les caractéristiques de l'espace polynomial.

Intermède

Rappelons qu'à l'époque de Galois, le problème était celui de la résolution par radicaux des équations polynomiales.
Cette question peut paraître aujourd'hui comme relativement « arbitraire » [24] mais elle semble pourtant plutôt « naturelle » : résoudre par radicaux, c'est très exactement dégager le nom algébrique de chaque racine. Et quoi en effet de plus « naturel » [25] quand une équation a délimité 5 nombres que de s'attacher à les nommer un par un avec les moyens algébriques du bord.
Deux petits exemples pour cela.

Formules par radicaux

Prenons l'exemple de cette formule compliquée [26] :

$$\sqrt[3]{11}\sqrt[5]{\frac{7+\sqrt{3}}{2}}+\sqrt[4]{1+\sqrt[3]{4}}$$

Comment s'analyse-t-elle en adjonctions successives ?
Comment se synthèse-t-elle en relations rationnelles ?

Posons pour cela :

- $\alpha=\sqrt[3]{11}$
- $\beta=\sqrt{3}$
- $\Longrightarrow \gamma=\sqrt[3]{\frac{7+\beta}{2}}$
- $\delta=\sqrt[3]{4}$
- $\Longrightarrow \varepsilon=\sqrt[4]{1+\delta}$

Le nombre initial s'écrira donc : $\alpha\gamma+\varepsilon$.
On y accède en 5 étapes : l'extension nécessaire de Q relève donc d'une tour de 5 adjonctions.

Notons que chaque étape peut s'écrire en relations polynomiales ordinaires :

- $\alpha^3=11$
- $\beta^2=3$
- $\Longrightarrow \gamma^3=(7+\beta)/2$
- $\delta^3=4$
- $\Longrightarrow \varepsilon^4=1+\delta$

Fonction $x^5+x^4-4x^3-3x^2+3x$

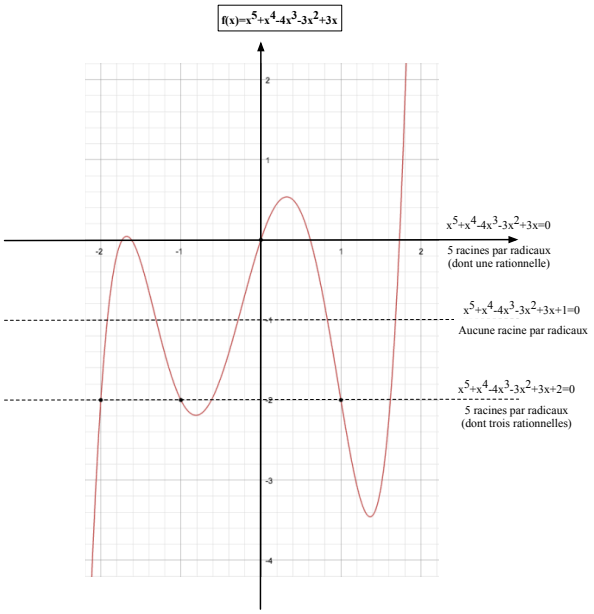
$f(x)=x^5+x^4-4x^3-3x^2+3x$ [$=x(x^2-3)(x^2+x-1)$]

- $x^5+x^4-4x^3-3x^2+3x=0 \Longrightarrow x(x^2-3)(x^2+x-1)=0 \Longrightarrow \{0, \pm\sqrt{3}, \frac{-1-\sqrt{5}}{2}, \frac{-1+\sqrt{5}}{2}\}$
- $x^5+x^4-4x^3-3x^2+3x=-2 \Longrightarrow (x+1)(x-1)(x+2)(x^2-x-1)=0 \Longrightarrow \{-2, \pm1, \frac{1-\sqrt{5}}{2}, \frac{1+\sqrt{5}}{2}\}$
- $x^5+x^4-4x^3-3x^2+3x=10 \Longrightarrow (x-2)(x^4+3x^3+2x^2+2x+5)$

mais $x^5+x^4-4x^3-3x^2+3x=-1 \Longrightarrow \{A\simeq-1,92 ; B\simeq-1,31 ; C\simeq-0,28 ; D\simeq0,83 ; E\simeq1,68\}$

---

[24] C'est par exemple le point de vue d'Olivier Debarredans le cours MOOC-FLOT de l'Ens (2014).
[25] au sens où les catégoriciens parlent de « transformations naturelles »…
[26] Stewart, p. 153



Polynôme $x^5+x^4-4x^3-3x^2+3x+1=0$

$$P(x)=x^5+x^4-4x^3-3x^2+3x+1=0$$ [27]

Ce polynôme s'avère irrésoluble par radicaux et ses 5 racines sont réelles.

$\Longrightarrow$ A≃-1,918986… ; B≃-1,309721… ; C≃-0,28463… ; D≃0,83083… ; E≃ 1,682507…

Il semble qu'on ait $E=4C^2+2D^2$ (calculs empiriques) mais ce n'est pas possible car le GG relie les 5 racines entre elles. Or si l'on avait bien $E=4C^2+2D^2$, de deux choses l'une :

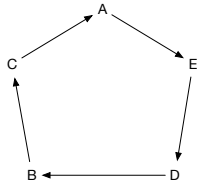
- soit cette relation ne vaut que pour ces 3 racines et pas pour A et B ; dans ce cas le GG serait séparable en 2+3 ;
- comme ce n'est pas le cas, cela voudrait donc dire que cette relation vaudrait également pour les autres, ce qui n'est pas possible car cette relation n'engendre que des nombres positifs ; or on sait que A, B et C sont des réels négatifs.

En fait, on a ici le « générateur » suivant : $x\mapsto x^2-2$ soit $P(x)=0 \Longrightarrow P(x^2-2)=0$

Donc $r'=r^2-2$:

$A = C^2-2 \simeq -1,92…$
$B = D^2-2 \simeq -1,31…$
$C = B^2-2 \simeq -0,28…$
$D = E^2-2 \simeq 0,83…$
$E = A^2-2 \simeq 1,68…$

Le GG n'ordonne donc pas les racines selon leur ordre numérique mais ainsi : A, E, D, B, C, soit :



Polynôme dual

On déduit de cela l'existence d'un polynôme P'(x) dual de P(x) :

$$Q(x)=P(x^2-2)=(x^2-2)^5+(x^2-2)^4-4(x^2-2)^3-3(x^2-2)^2+3(x^2-2)+1=x^{10}-9x^8+28x^6-35x^4+15x^2-1$$

On vérifie que

$$Q(x)=P(x^2-2)=P(x)P'(x) : x^{10}-9x^8+28x^6-35x^4+15x^2-1=(x^5+x^4-4x^3-3x^2+3x+1)(x^5-x^4-4x^3+3x^2+3x-1)$$

D'où le polynôme dual :

$$P'(x)=x^5-x^4-4x^3+3x^2+3x-1=0$$

dont les racines sont l'inverses de celles de P :

$\Longrightarrow$ -E=-1,68 ; -D=-0,83 ; -C=0,28 ; -B=1,31 ; -A=1,92

Ainsi

$$P'(x)=(x+A)(x+B)(x+C)(x+D)(x+E)$$

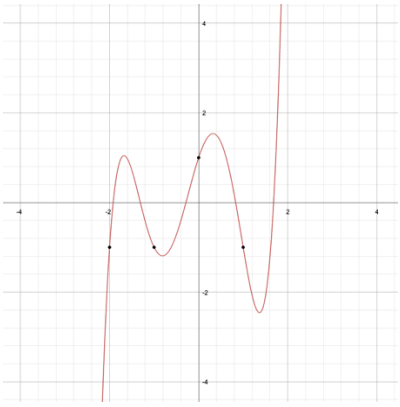
Au total

[27] Exemple de Connes

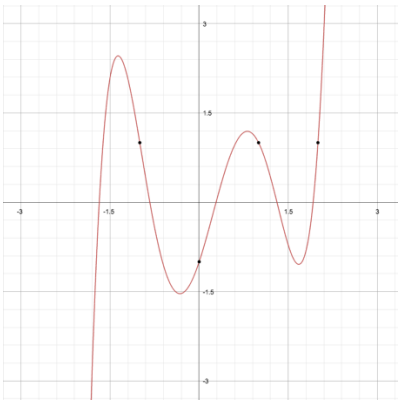
$Q(x)\cong(x\pm A)(x\pm B)(x\pm C)(x\pm D)(x\pm E)$ [Attention : soit tous les +, soit tous les -]

P/P' :

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



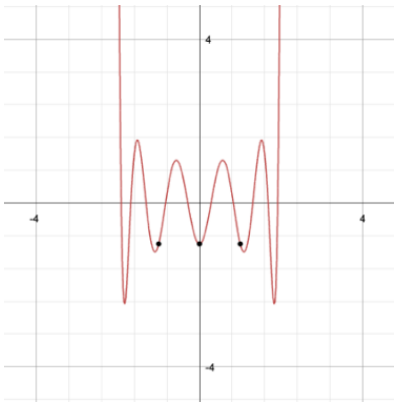
$x^5-x^4-4x^3+3x^2+3x-1$



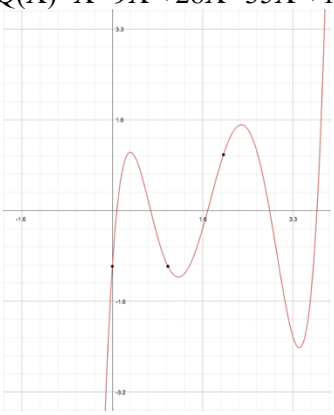
On peut procéder à un nouveau tour de piste car Q=P.P' est en x^2.

Q/Q'

$Q(x)=x^{10}-9x^8+28x^6-35x^4+15x^2-1$



Avec $X=x^2$: $Q(X)=X^5-9X^4+28X^3-35X^2+15X-1$



Q a pour racines les carrés des racines de P/P' :

$X^5-9X^4+28X^3-35X^2+15X-1=0 \Longrightarrow 0{,}08\ldots\ ;\ 0{,}69\ ;\ 1{,}715\ldots\ ;\ 2{,}83\ ;\ 3{,}68$ (carrés des racines de P)

Q' est à Q ce que P' est à P : racines inverses

$Q'(X)=X^5+9X^4+28X^3+35X^2+15X+1 \Longrightarrow -3{,}68\ ;\ -2{,}83\ ;\ -1{,}71\ ;\ -0{,}69\ ;\ -0{,}08$

Le générateur est désormais : $E^2=(A^2-2)^2$

R/R'

On déduit de Q.Q' un nouveau polynôme en $X^2=x^4$.

$$Q(X).Q'(X)=X^{10}-25X^8+184X^6-403X^4+155X^2-1$$

D'où à nouveau, en posant $y=X\hat{E}$ deux polynômes duaux :

$R(y)=y^5-25y^4+184y^3-403y^2+155y-1=0 \Longrightarrow 0{,}006\ ;\ 0{,}476\ ;\ 2{,}49\ ;\ 8{,}01\ ;\ 13{,}56$

$R'(y)=y^5+25y^4+184y^3+403y^2+155y+1=0 \Longrightarrow -13{,}56\ ;\ -8{,}01\ ;\ -2{,}49\ ;\ -0{,}476\ ;\ -0{,}006$

Le générateur est ici $E^4=(A^2-2)^4$

Famille

On engendre ainsi une famille de polynômes duaux :

	$x^5+x^4-4x^3-3x^2+3x+1$	$x^5-x^4-4x^3+3x^2+3x-1$	$x^{10}-9x^8+28x^6-35x^4+15x^2-1$
$A=C^2-2$	$A\simeq-1{,}92$; $B\simeq-1{,}31$; $C\simeq-0{,}28$; $D\simeq0{,}83$; $E\simeq1{,}68$	$-E\simeq-1{,}68$; $-D\simeq-0{,}83$; $-C\simeq0{,}28$; $-B\simeq1{,}31$; $-A\simeq1{,}92$	
	$x^5-9x^4+28x^3-35x^2+15x-1$	$x^5+9x^4+28x^3+35x^2+15x+1$	$x^{10}-25x^8+184x^6-403x^4+155x^2-1$
$A^2=(C^2-2)^2$	$0{,}08\simeq C^2$; $0{,}69\simeq D^2$; $1{,}715\simeq B^2$; $2{,}83\simeq E^2$; $3{,}68\simeq A^2$		
	$x^5-25x^4+184x^3-403x^2+155x-1$	$x^5+25x^4+184x^3+403x^2+155x+1$	
$A^4=(C^2-2)^4$	$0{,}006\simeq C^4$; $0{,}47\simeq D^4$; $2{,}49\simeq B^4$; $8{,}01\simeq E^4$; $13{,}56\simeq A^4$	$-13{,}56$; $-8{,}01$; $-2{,}49$; $-0{,}47$; $-0{,}006$	

Point de vue fonctoriel

Passons au mode d'exposition fonctoriel de la GT. C'est en fait celui adopté lors de l'atelier-Galois d'avril 2018.
Vous pouvez vous reporter aux dossiers alors établis à partir du livre de Stewart et du cours Ens de Debarre et Laszlo.
Je le présenterai aujourd'hui de manière très ramassée, en suivant les quelques intéressantes remarques… d'Alexandre Astruc dans le livre Évariste Galois [28] qui complète son film (25') de 1965 [29].

Centrons l'examen non plus sur l'existence du GG mais sur la théorie de sa résolution.

Cadrage général

Galois cerne son groupe de la manière suivante – je le cite en aménageant son texte à notre propos [30]:
« Soit une équation donnée. Il y aura toujours des permutations entre les racines (toutes ou une partie) formant un groupe (le groupe total ou un sous-groupe) jouissante de la double propriété suivante :

1. toute fonction à n variables des racines, invariable par les substitutions de ce sous-groupe, est rationnellement connue (c'est-à-dire que sa valeur numérique est fonction polynomiale des coefficients de l'équation et de quantités adjointes) ;
2. réciproquement, toute fonction des racines, déterminée rationnellement (au sens qu'on vient de préciser), est invariable par les substitutions de ce sous-groupe. »

Il y a donc, sur l'espace fonctionnel de toutes les fonctions polynomiales des n racines, une relation d'équivalence entre invariabilité (par permutations du GG) et résultats rationnels.

Prenons deux exemples .

- Soit $x^3-3x^2-2x+2=(x-1)(x^2-2)=(x-1)(x+\sqrt{2})(x-\sqrt{2})$.
  Quand une fonction polynomiale $f(A, B, C)=f(1, \sqrt{2}, -\sqrt{2})$ n'aura de résultats que rationnels ?
  Si, chaque fois qu'elle mobilise B, elle mobilise également C par produit BC :
  par exemple $25A+50BC+75A^2(BC)^5=25+50.2+75.2^5$ sera rationnel.
  À l'inverse une fonction du type $25A+50B+75C$ vaudra $25+50\sqrt{2}-75\sqrt{2}=25-25\sqrt{2}$ qui n'est pas rationnel.
  Les substitutions du GG sont donc celles qui font laissent A=1 inchangé et qui permutent les deux autres :

1	$\sqrt{2}$	$-\sqrt{2}$
1	$-\sqrt{2}$	$\sqrt{2}$

  On voit bien que, si on adjoint $\sqrt{2}$, alors la seule substitution laissant invariable tous les polynômes des racines à valeur dans $Q[\sqrt{2}]$ est l'identité.
- Soit $x^5+x^4-4x^3-3x^2+3x+1$ sans racines formulables par radicaux c'est-à-dire algébriquement.
  Les seules fonctions polynomiales f(A, B, C, D, E) qui auront des résultats rationnels seront les fonctions strictement symétriques qui peuvent être vues comme fonctions composées des 5 sommes coefficients-racines.
  On a en effet :
  $\sigma_0=A+B+C+D+E=-1$
  $\sigma_1=AB+AC+AD+AE+BC+BD+BE+CD+CE+DE=3$
  $\sigma_2=ABC+ABD+ABE+ACD+ACE+ADC+BCD+BCE+BDE+CDE=3$
  $\sigma_3=ABCD+ABCE+ABDE+ACDE+BDCE=-4$
  $\sigma_4=ABCDE=-1$
  D'où toutes les fonctions polynomiales à 5 variables sur les σ_j

Groupe

L'idée directrice de groupe algébrique est essentiellement celle d'un ensemble d'opérations tel que l'enchaînement de deux d'entre elles (leur « produit ») équivaut à une opération de l'ensemble. [31] La composition des opérations – ici des permutations - ne fait pas sortir de la famille des opérations.

---

[28] Flammarion, 1994
[29] https://www.youtube.com/watch?v=BAmhQle-uvA
[30] Voir le détail dans Connes (p. 5)
[31] Pour avoir le groupe, il faut bien sûr ajouter aux opérations l'opération neutre et, concomitamment, l'existence systématique d'opérations inverses.

Cette endogénéité ne va pas de soi : enchaîner plusieurs opérations de même type peut conduire à une opération résultante d'un tout autre type. Songez aux effets de seuil où l'opération réitérée en vient à muter de nature (voir le verre qui finit par déborder par ajouts répétés d'une goutte d'eau).

Sous-groupe

Il y a ensuite l'idée, assez naturelle, de sous-groupe (un groupe dans le groupe).

Sous-groupe distingué

Il y a ensuite l'idée la plus décisive : celle de sous-groupe distingué, ou normal.
C'est un sous-groupe stable par conjugaison (dans l'action de groupe) : H est distingué dans G ssi $\forall h \in H$: $gH=Hg$.

Ian Stewart en donne une caractérisation amusante : c'est un groupe « syndical » en ce que si l'un des éléments a une propriété, alors tous l'ont aussi.
Autrement dit ; si vous attrapez un élément, vous ne pouvez qu'attraper tous les autres à la fois.
C'est à nouveau l'image de multiples monozygotes : si vous en caractérisez un, vous caractérisez tout autant chacun d'eux.
Un groupe distingué constitue donc un groupe entièrement solidaire : vous ne pouvez distinguer aucun élément plutôt qu'un autre (c'est sans doute pour cela qu'on l'appelle tel : on ne peut distinguer que l'ensemble du groupe, non certains de ses éléments).
Attention : c'est une notion relative ! Un sous-groupe est distingué relativement au groupe dont il est le sous-groupe, c'est-à-dire relativement au corps sur lequel le groupe opère. À nouveau l'indistinction est relative au type d'existence prise en compte dans la situation, ici dans le corps de définition du groupe.

Groupe-quotient

Cette idée est particulièrement importante car le SG distingué permet de définir un groupe-quotient : en effet, le fait que le SG distingué soit stable par conjugaison permet de définir une relation d'équivalence sur G. On pose alors pour x et $y \in G$: xRy ssi $xy^{-1} \in H$.
On note G/H l'ensemble des classes d'équivalence = le groupe-quotient.

Correspondance de Galois

On a ainsi constitué l'opération élémentaire de la correspondance de Galois [CG], le moteur qui la crante (je rappelle que la CG est une correspondance fonctorielle c'est-à-dire qu'elle marche sur deux jambes - les corps et les groupes – et que cette marche est coordonnée par l'anneau des polynômes).

Opération élémentaire

Quotientage-distinction du groupe ∇G

↕ par division « idéale » des anneaux

Adjonction-extension du corps ΔK

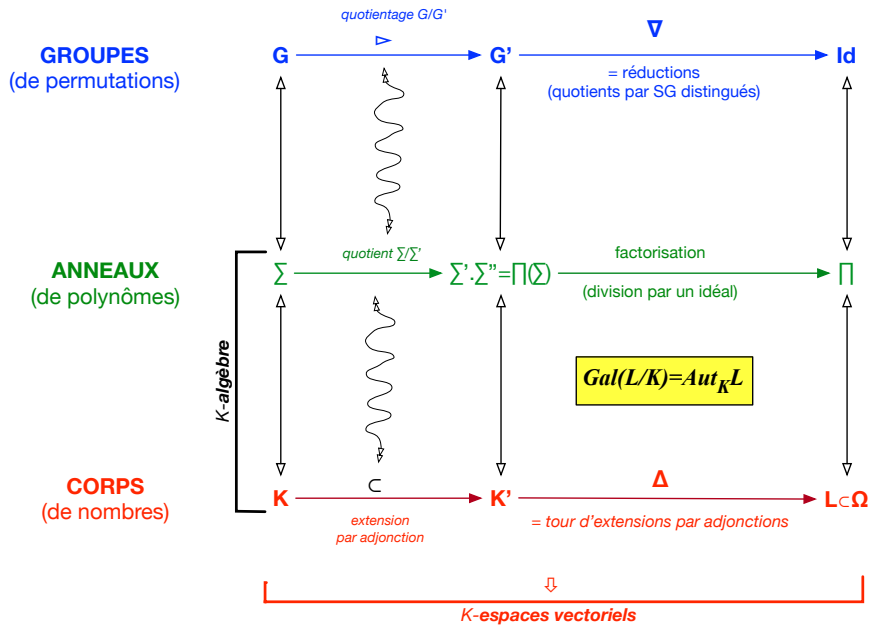
Groupes simples/composés

D'où la distinction entre groupes simples et groupes composés : un groupe est simple si ses seuls sous-groupes distingués sont {1} et G. Sinon, il est composé. Dans ce cas, on le décompose en groupes simples. Puis on réduit l'ordre du groupe simple par adjonctions.

Réduction vers Id

La résolution de Galois va consister à réduire progressivement l'ordre du sous-groupe distingué par judicieuses adjonctions en sorte d'arriver, si possible, au groupe identité Id où toutes les racines sont devenues rationnellement distinguables et où la seule permutation rendant invariable les polynômes sur ce corps étendu est la permutation identité.
Le GG sera résoluble s'il existe un processus distingué noté ∇G, c'est-à-dire une suite décroissante de sous-groupes allant jusqu'à Id telle que chaque sous-groupe est distingué dans le précédent et que le groupe quotient du groupe par le sous-groupe distingué est commutatif.

$G=G_0 \triangleright G_1 \triangleright G_2 \triangleright \ldots \triangleright G_n=Id$
avec G_i distingué dans G_{i-1}
et G_{i-1}/G_i commutatif.



III. Prolongements mathématiques

Passage à l'infini : les séries formelles

Peut-on passer de $\sum$ à $\prod$ quand la somme polynomiale devient infinie ? On parle alors de « séries formelles ». On sait qu'une telle série formelle peut alors être :

- convergente
- divergente ($\pm\infty$) : 1+2+3+4…
- indéfinie (1-1+1-1+1…)

Exemples de séries convergentes :

- pour 0<x<1 : $\sum x^n = \frac{1}{1-x}$
- $\sum \frac{x^n}{n!} = 1+x/1! + x/2! + \ldots = e^x$
- $x-x^3/3! + x^5/5! - x^7/7!\ldots = \sin(x)$
- $1-x^2/2! + x^4/4! - x^6/6!\ldots = \cos(x)$

Lorsque la série est convergente, peut avoir $\sum \Longrightarrow \prod$? A-t-on par exemple $\sin(x)=\prod(x-r_j)$?
Il semblerait qu'on puisse l'avoir, dans certains cas, mais alors le $\prod$ en question, convergent vers un nombre non rationnel et non algébrique, ne serait plus unique et pourrait même comporter une infinité de possibilités. Un théorème de Hurwitz traiterait de cette situation. [32]

Le groupe de Galois différentiel

Cf. équation algébrique $\Longrightarrow$ équation différentielle (linéaire) où l'inconnue est une fonction.
Principal résultat : il y a dans ce cas 3 (et 3 seulement) types d'ambiguïtés galoisiennes (c'est-à-dire d'éléments du groupe de Galois différentiel) [33] :

- la monodromie (on ne revient pas au point de départ après avoir tourné autour d'une singularité),
- le recalibrage des exponentielles (au voisinage d'une singularité)
- les ambiguïtés de Stokes (également au voisinage d'une singularité).

Les perfectoïdes

Cf. les nombres p-adiques : même structure d'espace et de groupe avec les polynômes… [34]

---

[32] Merci à Yves André pour cette indication.
[33] Voir Yves André : *Idées galoisiennes* (leçon mamuphi).
[34] Voir http://images.math.cnrs.fr/Perfectoides.html

IV. R*ai*sonances

Évariste

Sa vie

25 octobre 1811 – 31 mars 1832

Année scolaire	Âge	Classe	Établissement	
1823-1824	12	Quatrième	Louis-le-Grand	
1824-1825	13	Troisième		
1825-1826	14	Seconde		
1826-1827	15	(redoublement !)		
1827-1828	16	Première		
1828-1829	17	Terminale		
1829-1830	18		Normale	
1830-1831	19		Normale | Prison	
1831-1832	20		Prison	

Sa mort, une équation à 5 inconnues !

- Raison du duel ?
- Qui fut la coquette ?
- Qui fut son adversaire ?
- Qui furent ses deux témoins ? [deux inconnus « conjugués » !]

Générales

Modernités

1. MI : Systématisation (Dedekind…)
2. MII : Généralisation formelle (Emil Artin…)
3. MIII : Extension (Grothendieck…)

« *Tout processus de généralisation s'accompagne d'une subdivision en concepts distincts qui se trouvaient confondus dans la situation particulière d'abord envisagée. En mathématiques, la crainte que généralité et banalité aillent de pair est absolument injustifiée ! […] La généralisation d'un concept s'accompagne souvent d'une différenciation en deux ou plusieurs aspects jusque-là non distingués et qui appellent à leur tour des concepts spécifiques.* » Hourya Sinaceur [35]

Comme l'indique Hourya Sinaceur, une généralisation ne procède pas par fusion/confusion de notions mais produit tout au contraire une division/séparation/distinction de notions jusque-là mal discernées.

Néoclassicisme / transmodernité

Cf. Connes d'un côté ⟹ continuité par point de vue fonctionnel…
Cf. Zalamea de l'autre ⟹ sauts mais alors quelles continuités ?

De la fonctionnalité à la Fonctorialité

Extension de la fonctionnalité classique (cf. la notion de *fonction* est au cœur de l'analyse) : la correspondance s'étend des objets aux morphismes qui les relient au terme de quoi la correspondance se fait entre structures et non plus entre objets.

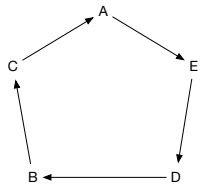
De la collection constituée au collectif constituant…

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

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

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

[35] *Corps et modèles* (pp.383-384 ; 398)

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

Solidarité

Manière de renommer symétrie ou ambiguïté…

À partir de 5…

Le collectif constituant commence à 5. [36]
En-dessous, le collectif est constitué.

Musique

L'écoute

l'écoute entre l'amalgame de l'oreille (∑) et l'algèbre de la partition (∏) ?
Et : $\frac{\nabla G}{\Delta K} \equiv \frac{\Delta\,(\acute{E}criture \rightarrow Partition)}{\nabla\,(Perception \rightarrow \acute{E}coute)}$?

Wagner

moins le groupe des différents leitmotivs qu'un seul leitmotiv comme groupe de ses différentes variantes…

Politique

Le groupe politique ?

Lien entre modernité galoisienne et modernité marxiste !

Galois-Marx-Wagner : 3 militants politiques révolutionnaires porteurs de nouvelles conceptions du collectif.

Cf. la question de l'organisation comme question centrale de la politique. ⟹ Marx, galoisien ?
L'organisation communiste : un groupe irréductible sans sous-groupes distinguables ? Cf. sa solidarité constituante, qui se nomme « camaraderie » ; cf. le fait que les individus s'y intègrent le plus souvent sous pseudonyme.

Grouper l'humanité ?

Groupes infinis ⟹ séries formelles…

Arts

Voir le projet *Douze* (Blok) pour « grouper » musique, théâtre et cinéma et non pas les totaliser en « œuvre d'art totale »…

Montage cinématographique

Le montage du cinéma serait-il une manière de « grouper » ses différentes composantes ?

***

[36] En langue russe, le pluriel commence à 5 et le singulier concerne les nombres{1, 2, 3, 4}.
Il y a de nombreuses langues avec un duel (le Grec, l'Arabe…). Il y a quelques langues avec un triel et il y en aurait (le *Sursurunga* de Papouasie-Nouvelle-Guinée) avec le jeu complet : {singulier, duel, triel, quatriel, paucal (peu), pluriel (beaucoup)}.
Notons aussi le cas où la langue distingue un nom collectif qui n'est pas le pluriel (Arabe par exemple). D'où, parfois, le *singulatif* qui est l'unité de ce nom collectif (quelque chose en français comme « un membre du troupeau bovin ou ovin »). Singulatif s'oppose alors à collectif comme singulier s'oppose à pluriel…