Eine kleine Galoistheorie : une introduction en mots artistiques aux découvertes d'Evariste Galois, mathématicien mozartistique

Douglas Hofstadter(*)

Introduction

C'est la première fois que je donne cette conférence, alors je me sens un peu nerveux et j'espère que vous m'en excuserez.
Je vais parler *principalement* d'Évariste Galois et de sa théorie mais je vais aussi parler un peu du parcours de la découverte en mathématiques, c'est-à-dire du fonctionnement de la pensée humaine ; pour cela, je voudrais commencer avec une citation de Henri Poincaré sur les analystes et leurs très très longs calculs :

> « Croira-t-on … qu'ils ont toujours marché pas à pas, sans avoir la vision du but qu'ils voulaient atteindre ?
> Il a bien fallu qu'ils devinassent le chemin qui y conduisait, et pour cela ils ont eu besoin d'un guide.
> Ce guide, c'est d'abord l'analogie. »

Ceci va être un des fils conducteurs de cette conférence, c'est-à-dire l'idée que l'analogie, c'est ce qui compte en mathématiques.
Nous allons aborder le sujet de la théorie de Galois en parlant de ce qui a précédé le développement de cette théorie : la résolution des équations polynomiales, à savoir :
– l'équation quadratique qui a été résolue(1) par Al-Khwarizmi vers 800 ;
– puis des génies italiens, au début et vers le milieu du XVI^{e} siècle, del Ferro, Tartaglia, Cardan, Bombelli ont découvert la solution de l'équation cubique ;
– Cardan et son assistant Ferrari ont également développé la solution de l'équation quartique.

Tout le monde voulait trouver quelque chose *d'analogue* pour l'équation quintique et pour toutes les autres équations et voulait utiliser les clés les plus simples pour ouvrir toutes les portes. Ces clés sont les radicaux : on prend les équations polynomiales les plus simples possibles : $x^2 - a = 0$, $x^3 - a = 0$, etc. dont les solutions sont des racines (on tient pour acquis que l'on peut toujours prendre une racine n-ième d'un nombre donné). L'idée (et l'espoir) était donc de résoudre toutes les équations polynomiales à l'aide de radicaux.
Nous pouvons dire que *l'analogie* a joué ici un vilain tour (la force fourvoyante de l'analogie) : l'équation quadratique se résout avec des racines quadratiques(2), la

(*) Indiana University. dughof@indiana.edu
(1) En réalité, cette équation avait été résolue longtemps auparavant, mais la résolution a été formalisée par Al-Khwarizmi.
(2) Racine quadratique : racine carrée.

résolution de l'équation cubique utilise des racines cubiques et des racines quadratiques, l'équation quartique n'utilise pas de racine quatrième mais des racines quadratiques et cubiques emboîtées.
On pense naturellement que cette progression va continuer mais c'est un espoir … naïf ! Cela ne marche pas et cela a été découvert par Ruffini en Italie, puis Abel et enfin Galois, mais c'est ce dernier qui a vraiment tout compris.

La théorie de Galois

C'est une théorie de *symétries non visuelles*, qui sont toutes des cousines de la conjugaison complexe qui est une sorte de réflexion et qui est, elle, très visuelle. Nous allons commencer avec la conjugaison complexe.

La conjugaison complexe

Prenons l'équation polynomiale $x^2 + 1 = 0$ dont les deux racines sont i et $-$i ; ces racines ne se trouvent pas sur l'axe des réels mais sur l'axe[3] des y ; ces racines sont dites « conjuguées[4] ».
Commençons donc avec le premier corps, celui des nombres réels ; il n'y a naturellement pas de racines de cette équation, nous devons ajouter quelque chose aux réels : les deux racines « magiques » sont i et $-$i. Cela donne un autre corps dont l'élément générique est $a + b$i où a et b sont des nombres réels. $\mathbb{C}$, le corps des nombres complexes, est *bidimensionnel* par rapport à $\mathbb{R}$.
La conjugaison complexe est un *automorphisme* du plan complexe $\mathbb{C}$: elle respecte l'addition et la multiplication.

$$\overline{x+y} = \overline{x} + \overline{y},\ \overline{xy} = \overline{x}\,\overline{y},\ x \in \mathbb{C},\ x \in \mathbb{C}.$$

Le conjugué de la somme est la somme des conjugués ; de même, le conjugué du produit est le produit des conjugués (la conjugaison complexe est donc un isomorphisme pour l'addition et pour la multiplication).
Il s'agit d'une symétrie tout à fait géométrique et visuelle, mais c'est aussi, *en même temps*, deux isomorphismes (de l'addition et de la multiplication).
La théorie de Galois a à voir avec des choses très semblables, des *analogues* avec d'autres corps, mais où tout n'est pas visuel.

Première analogie

Nous allons faire une première *analogie* avec la conjugaison complexe ; nous partons d'un autre corps, celui des nombres rationnels ($\mathbb{Q}$) qui est un sous-ensemble de la droite des réels.
Un **corps** est un ensemble de nombres avec 0 et 1 où l'addition, la multiplication, la soustraction et la division sont toujours possibles (sauf la division par 0, bien sûr).
Voici la droite des rationnels :

(3) Diagramme d'Argand : découverte faite par plusieurs personnes, y compris Argand en France, et qui consiste à mettre i et $-$i sur un autre axe que celui des réels.
(4) Des racines conjuguées d'une équation sont des racines qui sont *en même temps* racines de la *même* équation polynomiale irréductible dans le corps donné.

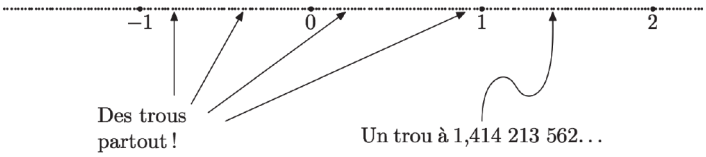


FIG. 1 – La droite des rationnels

Évidemment, ce n'est pas vraiment une droite, car il y a plein de trous...

Nous allons maintenant « inventer » des nombres « magiques » qui s'appellent $\sqrt{2}$ et $-\sqrt{2}$ et qui sont situés quelque part sur la droite des réels ; il s'agit ici aussi de deux racines conjuguées car ce sont des racines de la même équation : $x^2 - 2 = 0$.

Lorsque nous ajoutons $\sqrt{2}$ à $\mathbb{Q}$, nous obtenons un corps[5] très semblable au corps des nombres complexes et dont l'élément générique est $a + b\sqrt{2}$ (où a et b sont des rationnels) ; il s'agit encore une fois d'un sur-corps qui est *bidimensionnel* par rapport à $\mathbb{Q}$. La différence, c'est que nous ne pouvons pas faire un graphique, un diagramme ou un dessin à deux dimensions. Pourquoi ? Parce que, si nous voulons respecter les distances sur la droite, il faudrait qu'il y ait un homéomorphisme[6] qui relie la droite des réels avec le plan, donc entre deux espaces topologiques de dimensions différentes, et ceci n'est pas possible. Nous partons donc d'un corps « incomplet » par rapport à une équation polynomiale, nous lui ajoutons des racines « magiques » et nous obtenons un corps étendu qui a une certaine dimension par rapport au corps de départ.

Corps incomplet	Équation irrésoluble	Racines « magiques »	Corps étendu
$\mathbb{R}$	$x^2 + 1 = 0$	$\pm i$	$\mathbb{R}(i) = \{x + iy\}$ $x, y \in \mathbb{R}$
$\mathbb{Q}$	$x^2 - 2 = 0$	$\pm\sqrt{2}$	$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2}\}$ $a, b \in \mathbb{Q}$

TAB. 1 – Quelques corps étendus

Une équation quartique

Partons de l'équation quartique :

$$x^4 - x^2 - 2 = 0 \qquad (1)$$

Il s'agit d'une équation atypique car elle est trop simple pour être tout à fait générale ; elle se factorise en deux polynômes quadratiques :

$$x^4 - x^2 - 2 = (x^2 + 1)(x^2 - 2).$$

Les racines « magiques » sont : i, $-i$, $\sqrt{2}$ et $-\sqrt{2}$.

L'élément *générique* du corps étendu est $a + bi + c\sqrt{2} + di\sqrt{2}$ où a, b, c et d sont tous rationnels. Sa dimension est 4 par rapport à $\mathbb{Q}$.

(5) C'est un corps *dénombrable*, alors que $\mathbb{C}$ est non dénombrable.
(6) Correspondance continue.

Mais nous pouvons également considérer ce corps comme une extension de $\mathbb{Q}(i)$ et ayant comme élément générique $(a + bi) + (c + di)\sqrt{2}$, donc de dimension 2 par rapport à $\mathbb{Q}(i)$.

Ou comme une extension de $\mathbb{Q}\left(\sqrt{2}\right)$ et ayant comme élément générique

$$\left(a+c\sqrt{2}\right)+\left(b+d\sqrt{2}\right)\mathrm{i},$$

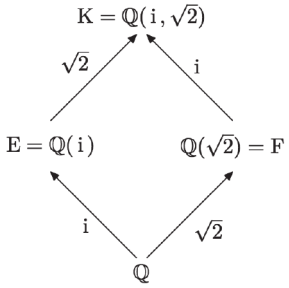
également de dimension 2 par rapport à $\mathbb{Q}\left(\sqrt{2}\right)$.

Nous pouvons résumer ceci dans le diagramme suivant :

Extension	Membre générique	Dimension
$\mathbb{R} \longrightarrow \mathbb{C}$	$x + \mathrm{i}\,y$ $(x,\ y \in \mathbb{R})$	2
$\mathbb{Q} \longrightarrow \mathbb{Q}(\sqrt{2})$	$a + b\sqrt{2}$ $(a,\ b \in \mathbb{Q})$	2
$\mathbb{Q} \longrightarrow \mathbb{Q}(\mathrm{i}, \sqrt{2})$	$a + b\mathrm{i} + c\sqrt{2} + d\mathrm{i}\sqrt{2}$ $(a,\ b,\ c,\ d \in \mathbb{Q})$	4

TAB. 2 – Dimension d'extensions par rapport au corps de départ

Nous pouvons également dessiner le treillis avec les deux corps intermédiaires :



$$[\mathrm{K} : \mathbb{Q}] = 4 = [\mathrm{K} : \mathrm{E}][\mathrm{E} : \mathbb{Q}] = 2 \times 2 = [\mathrm{K} : \mathrm{F}][\mathrm{F} : \mathbb{Q}] = 2 \times 2$$

FIG. 2 - Treillis de décomposition de $\mathbb{Q}\left(\mathrm{i}, \sqrt{2}\right)$

Considérons maintenant les analogues (car il y en a plusieurs) de la conjugaison complexe dans ce corps étendu K = $\mathbb{Q}\left(\mathrm{i}, \sqrt{2}\right)$ qui est de dimension 4 par rapport à $\mathbb{Q}$.

Nous pouvons déjà remplacer i par –i (restriction de la conjugaison complexe) ; nous pouvons également remplacer $\sqrt{2}$ par $-\sqrt{2}$:

$$\mathrm{V}\left(a+b\mathrm{i}+c\sqrt{2}+d\mathrm{i}\sqrt{2}\right)=a-b\mathrm{i}+c\sqrt{2}-d\mathrm{i}\sqrt{2},$$

$$\mathrm{H}\left(a+b\mathrm{i}+c\sqrt{2}+d\mathrm{i}\sqrt{2}\right)=a+b\mathrm{i}-c\sqrt{2}-d\mathrm{i}\sqrt{2}.$$

Mais il y a également une troisième conjugaison, celle obtenue en composant V et H :

$$\Pi = \mathrm{HV} = \mathrm{VH},$$
$$\Pi\left(a + b\,\mathrm{i} + c\sqrt{2} + d\,\mathrm{i}\sqrt{2}\right) = a - b\,\mathrm{i} - c\sqrt{2} + d\,\mathrm{i}\sqrt{2}.$$

Une analogie révolutionnaire de Galois

II traite les automorphismes comme s'ils étaient des nombres.

Il passe donc à un autre niveau d'abstraction et considère les phénomènes qui se passent à ce niveau comme des phénomènes normaux des mathématiques.
Il a le concept de « multiplication » des automorphismes et dresse une « table de multiplication » pour eux. Voici celle des automorphismes de K :

	I	V	H	Π
I	I	V	H	Π
V	V	I	Π	H
H	H	Π	I	V
Π	Π	H	V	I

FIG. 3 – Table de multiplication des automorphismes de K

où nous considérons toutes les conjugaisons de K qui laissent $\mathbb{Q}$ invariant (les trois conjugaisons déjà rencontrées et I, l'identité de K).
Nous reconnaissons ici la structure du groupe à quatre éléments communément appelé « groupe de Klein » (l'autre groupe à quatre éléments étant $\mathbb{Z}_4$).
Cette table possède des symétries évidentes qui frappent la vue.
Nous pouvons également représenter ce groupe de symétries comme les symétries d'une brique :

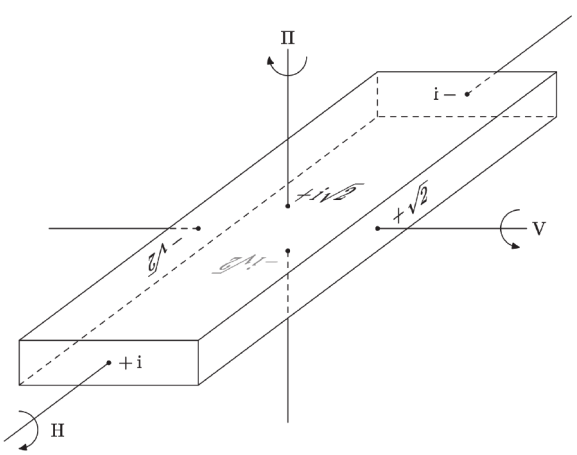
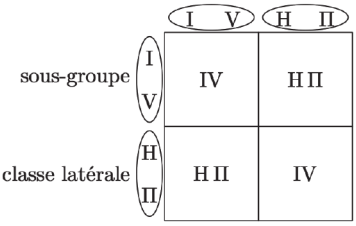


FIG. 4 – Les symétries d'une (algé)brique

Deuxième analogie révolutionnaire de Galois

Il traite les groupes et leurs sous-groupes comme s'ils étaient des nombres.

Il invente une sorte de « division » pour ces grandes structures abstraites.
Reprenons la table de multiplication précédente en rassemblant I et V d'une part, H et Π d'autre part (structure à gros grain) :



Nous reconnaissons ici la table de multiplication de $\mathbb{Z}_2$, le groupe cyclique d'ordre 2 :

	0	1
0	0	1
1	1	0

FIG. 5 – Table de multiplication de la structure à gros grain des automorphismes de K

Les diagrammes de Cayley

Ces diagrammes rendent visibles et tangibles les groupes même si, pour les groupes cycliques, qui jouent un rôle central dans la théorie de Galois, ce n'est pas très intéressant.
Voici les exemples les plus simples des diagrammes de Cayley.

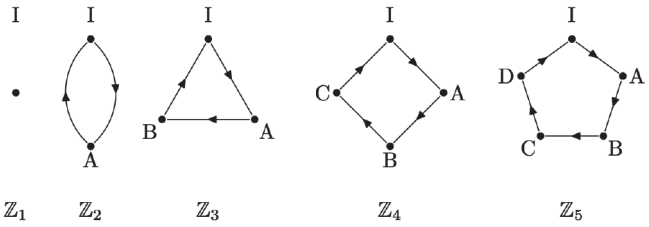


FIG. 6 – Diagrammes de Cayley de $\mathbb{Z}_1$, $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_4$ et $\mathbb{Z}_5$

Pour $\mathbb{Z}_1$, c'est trivial.

$\mathbb{Z}_2$ possède deux arcs, $\mathbb{Z}_3$ en possède trois, etc. I représente l'identité et la flèche représente la multiplication par A ; par exemple, dans $\mathbb{Z}_5$, I multiplié par A donne A, A multiplié par A donne B, B multiplié par A donne C, C multiplié par A donne D et D multiplié par A redonne I : A est un élément d'ordre 5.

Regardons maintenant le diagramme de Cayley du groupe de Klein (cf. Fig. 7).

C'est un groupe à quatre éléments. La multiplication par V est le générateur du sous-groupe {I,V} : si nous multiplions I par V, nous obtenons V ; si nous multiplions V par V, nous obtenons I ; si nous multiplions H par V, nous obtenons Π et si nous multiplions Π par V, nous obtenons H.
Le trait ondulé représente la multiplication par H.

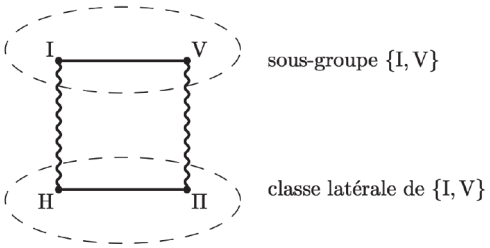


FIG. 7 – Diagrammes de Cayley du groupe de Klein

Cette figure représente donc le diagramme de Cayley du *petit* groupe de *Klein*. Ce groupe possède trois sous-groupes d'ordre 2 : {I,V}, {I,H} et {I,Π}. J'ai choisi de privilégier le sous-groupe {I,V} ; alors {H,Π} est appelée une *classe latérale*.

Comment visualiser le groupe quotient dans le cas du groupe de Klein? Ce qui nous laisse percevoir l'existence de groupes quotient, c'est l'existence de « câbles » qui relient le sous-groupe avec les classes latérales.

Dans le cas du groupe de Klein, c'est vraiment très banal :

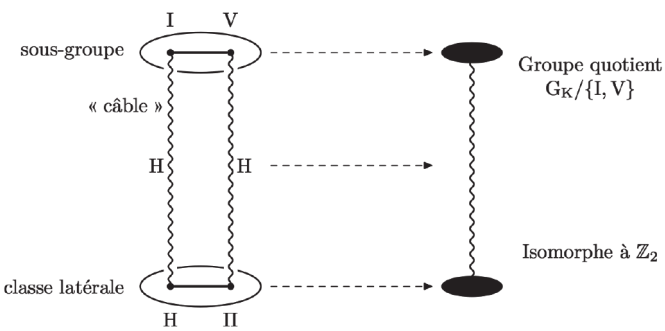


FIG. 8 – La structure à gros grain de G_K

Nous avons le sous-groupe {I,V}, nous avons l'existence d'un câble qui passe de ce sous-groupe à la classe latérale {H,Π}. Nous pouvons alors simplifier ce schéma : nous remplaçons le câble par un fil, le sous-groupe par un point et sa classe latérale par un autre point. Nous obtenons alors le diagramme de Cayley d'un groupe plus petit, isomorphe à $\mathbb{Z}_2$: il s'agit du groupe quotient obtenu en divisant le groupe de Klein G_K par son sous-groupe {I,V}.

Galois a eu ici une idée géniale : diviser un groupe par un de ses sous-groupes.

Troisième analogie révolutionnaire de Galois

Il crée deux treillis de structures totalement différentes et en observe l'isomorphie parfaite !

Voici le treillis des sous-groupes de G_K, où nous pouvons diviser G_K par chacun des sous-groupes {I,V}, {I,H}, {I,Π} et, de même, nous pouvons diviser chacun de ces sous-groupes par {I}.

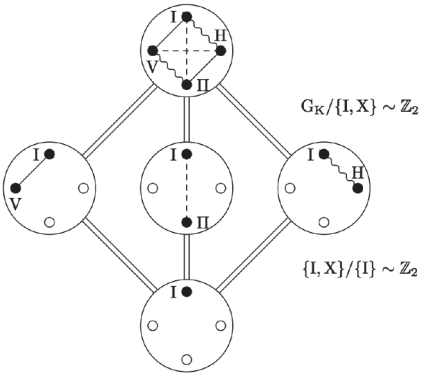


FIG. 9 – Treillis des sous-groupes de G_K

Je vous rappelle que G_K est le groupe de tous les automorphismes (conjugaisons) possibles du corps de décomposition de notre polynôme quartique.

Regardons maintenant le treillis des extensions de corps entre $\mathbb{Q}$ et $\mathbb{Q}\left(i,\sqrt{2}\right)$:

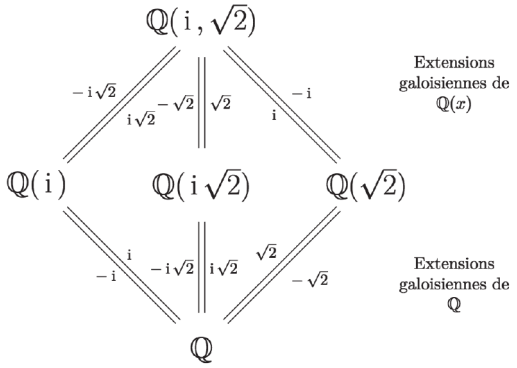


FIG. 10 – Treillis des extensions de corps entre $\mathbb{Q}$ et $\mathbb{Q}\left(i,\sqrt{2}\right)$

Il y a trois façons de monter de $\mathbb{Q}$ à un corps intermédiaire (soit $\mathbb{Q}(i)$, soit $\mathbb{Q}\left(i\sqrt{2}\right)$, soit $\mathbb{Q}\left(\sqrt{2}\right)$) ; puis, à partir d'un corps intermédiaire, nous pouvons ajouter encore d'autres éléments pour arriver au corps de décomposition entier. Nous nous rendons compte qu'il y a une ressemblance très frappante entre ce treillis d'extensions de corps et le treillis des sous-groupes de G_K.
Ce n'est évidemment pas une coïncidence mais nous verrons qu'il y a une subtilité que je n'ai pas mentionnée : il faut en réalité faire une rotation de 180° pour avoir l'isomorphie que Galois a découverte.

Le cas révélateur de l'équation cubique

Si une équation *quadratique* a deux « conjugaisons algébriques » (Ψ et I) et si une équation *quartique* en a quatre (I, V, H et Π), alors combien y en a-t-il pour une équation cubique ?

Non, pas trois ! Six !

Pourquoi ? Parce que je vous ai volontairement fourvoyés : l'équation quartique que j'ai choisie est un cas dégénéré et, en général, il y a beaucoup plus que quatre conjugaisons (symétries) pour une équation quartique.
L'équation cubique classique a six automorphismes ; nous allons voir pourquoi dans un cas particulier(7).
Considérons l'équation cubique

$$x^3 - 2 = 0 \qquad (2)$$

J'appelle χ, Ξ et Θ les trois racines. χ est la racine réelle :

$$\chi = \sqrt[3]{2} \simeq 1,259\,921\ldots,$$
$$x^3 - 1 = (x - \chi)\left(x^2 + \chi x + \chi^2\right).$$

Il reste une équation quadratique à résoudre :

$$x^2 + \chi x + \chi^2 = 0. \qquad (3)$$

Les deux solutions de cette dernière sont : $\begin{matrix}\Xi = \omega\chi \\ \Theta = \omega^2\chi\end{matrix}$ où $\omega = -\frac{1}{2} + \frac{\mathrm{i}}{2}\sqrt{3}$ (racine cubique de 1).
La solution χ a un degré 3, alors que les solutions de l'équation quadratique (3) ont un degré 2 ; et si nous multiplions 3 par 2, nous obtenons 6 : c'est la raison pour laquelle il y a 6 automorphismes.
Regardons cela plus géométriquement dans le plan complexe :

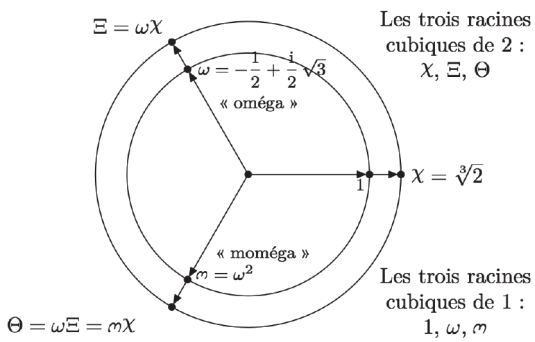


FIG. 11 – Représentation géométrique des racines de $x^3 - 2$

Si nous voulons construire le corps de décomposition de cette équation, nous avons deux manières de procéder :

– soit nous ajoutons d'abord $\sqrt[3]{2}$ $(= \chi)$ puis ω.
En ajoutant d'abord χ, nous obtenons un corps intermédiaire $\mathrm{U} = \mathbb{Q}(\chi)$ qui a la dimension 3 par rapport à $\mathbb{Q}$ car l'élément générique de U est $a + b\chi + c\chi^2$ $(\chi^3 = 2)$ avec a, b et c éléments de $\mathbb{Q}$.
Puis, en ajoutant ω, nous obtenons le corps de décomposition K dont le terme

(7) Mais le raisonnement est tout à fait général.

générique est $u + v\omega$ (u et v éléments de U). ω est un élément quadratique, donc la dimension du corps de décomposition par rapport à U est égale à 2. En multipliant, nous obtenons bien une dimension de 6 du corps de décomposition par rapport à $\mathbb{Q}$;

– soit nous ajoutons d'abord ω puis χ.

L'ajout de ω nous donne un corps intermédiaire $W = \mathbb{Q}(\omega)$ qui est de dimension 2 par rapport à $\mathbb{Q}$ (terme générique $a + b\omega$ avec a et b éléments de $\mathbb{Q}$).

Ensuite, l'ajout de χ nous donne K qui est de dimension 3 par rapport à W (terme générique $w + x\chi + y\chi^2$ avec w, x et y éléments de W

Nous obtenons la même chose, mais en ne passant pas par le même chemin.

Nous pouvons résumer ceci dans le diagramme suivant :

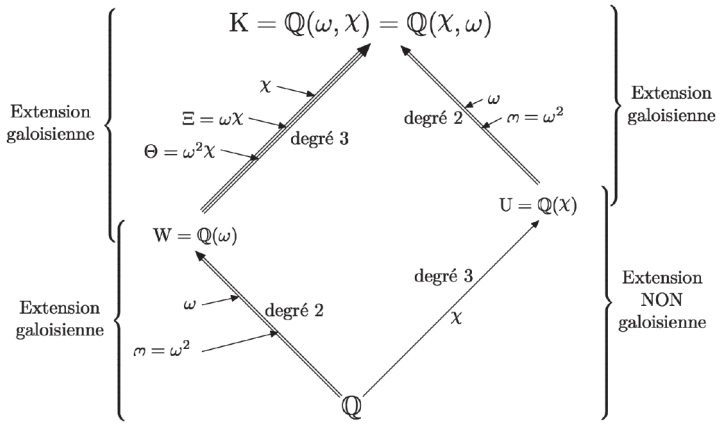


FIG. 12 – Les deux chemins pour passer de $\mathbb{Q}$ à K

Par le chemin de gauche, en ajoutant d'abord ω, nous passons de la droite des réels au plan complexe ; ensuite, en ajoutant χ, comme nous pouvons le multiplier par ω, **toutes les racines montent en même temps** (en passant de W à K).

En revanche, par le chemin de droite, en ajoutant χ, nous n'ajoutons qu'un nombre réel à $\mathbb{Q}$, donc ses compagnons (Ξ et Θ) ne peuvent pas monter en même temps (U est un sous-corps de $\mathbb{R}$).

Ceci nous conduit à définir une **extension galoisienne** :

Une extension galoisienne est une extension où toutes les racines conjuguées montent ensemble.

Remarque : ce que nous avons fait avec χ, nous aurions pu en faire autant avec Ξ ou Θ, les racines conjuguées de χ ; nous aurions obtenu deux autres extensions **non** galoisiennes, isomorphes à $U = \mathbb{Q}(\chi)$; ces extensions sont des extensions de $\mathbb{Q}$ *conjuguées*.

Voici un diagramme résumant tout ceci :

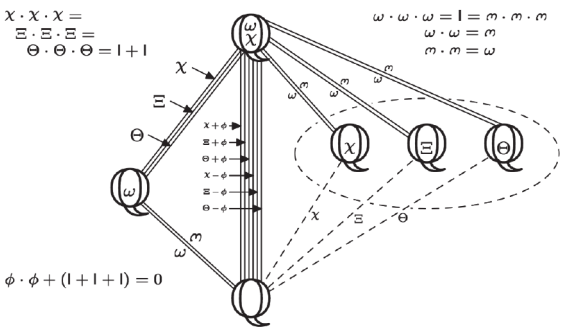


FIG. 13 – Diagramme des extensions de $\mathbb{Q}$

Nous avons même la possibilité d'ajouter directement à $\mathbb{Q}$ des nombres comme $\chi \pm \phi$ ou $\Xi \pm \phi$ ou $\Theta \pm \phi$ (où ϕ vérifie $(\phi^2 + 3 = 0)$ et nous obtenons directement[8] $\mathbb{Q}(\omega,\chi)$. Je n'en parlerai pas plus longuement.

Pour une cubique générale avec coefficients rationnels, les racines ont la forme

$$\sqrt[3]{r+\sqrt{\Delta}} + \sqrt[3]{r-\sqrt{\Delta}}$$

où r et Δ sont rationnels, et sont fonctions des coefficients du polynôme cubique. Nous avons donc affaire, en général, à une extension *quadratique* (par $\sqrt{\Delta}$) et aussi une extension *cubique* (par $\sqrt[3]{\cdots}$), ce qui a pour conséquence que le corps de décomposition d'une cubique a, en général, une dimension de **6** par rapport à $\mathbb{Q}$.

Regardons maintenant les symétries du corps $K = \mathbb{Q}(\chi,\Xi,\Theta) = \mathbb{Q}(\chi,\omega)$:

– nous pouvons tout d'abord échanger ω avec ϖ (conjugaison complexe) ; c'est, en même temps, l'échange entre les deux racines Ξ et Θ ; notons « f » cette symétrie ;
– nous avons une autre symétrie, que nous noterons « P » : c'est la rotation cyclique (permutation circulaire) où χ devient Ξ, Ξ devient Θ, et Θ devient χ. Il s'agit d'automorphismes de K qui laissent fixe le sous-corps $\mathbb{Q}$.

Pourquoi y a-t-il des symétries d'une cubique ? Parce que les racines sont indifférenciables algébriquement.

Oui, mais pourquoi cela? Parce que

(8) Les valeurs $\chi \pm \phi$, $\Xi \pm \phi$, $\Theta \pm \phi$ sont en réalité les six solutions de l'équation du sixième degré :

$$x^6 + 9x^4 - 4x^3 + 27x^2 + 36x + 31 = 0.$$

Cette équation, étudiée par Lagrange et Vandermonde, est appelée en anglais « *the resolvent equation of the given cubic equation* » ; ce n'est pas une équation typique du sixième degré car son groupe de Galois est S_3 alors que le groupe de Galois d'une équation générale du sixième degré est S_6. En revanche, ses six racines montent en même temps dès que nous en ajoutons une à $\mathbb{Q}$.

$$(x-a)(x-b)(x-c)=0$$

devient

$$x^3-\underbrace{(a+b+c)}_{\uparrow}x^2+\underbrace{(ab+bc+ca)}_{\uparrow}x-\underbrace{abc}_{\uparrow}=0$$

invariant pour $a \leftrightarrow b$, $b \leftrightarrow c$, $c \leftrightarrow a$,

ainsi que par les permutations circulaires

$a \to b \to c \to a$ et $a \leftarrow b \leftarrow c \leftarrow a$

Nous pouvons voir graphiquement en quoi consistent ces symétries :

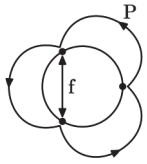


FIG. 14 – Représentation graphique des six permutations de trois objets

Un échange (f) et une rotation cyclique (P) suffisent pour générer toutes (6) les permutations possibles de 3 objets.

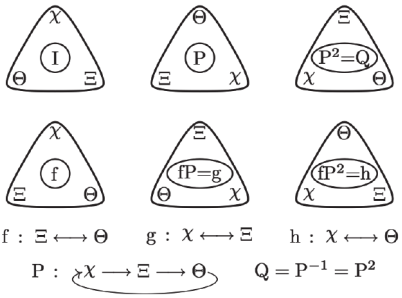


FIG. 15 – Une autre représentation des six permutations de trois objets

Regardons maintenant la table de multiplication de ces six permutations :

		I	P	Q	f	g	h
sous-groupe	I	I	P	Q	f	g	h
	P	P	Q	I	g	h	f
	Q	Q	I	P	h	f	g
classe latérale	f	f	h	g	I	Q	P
	g	g	f	h	P	I	Q
	h	h	g	f	Q	P	I

FIG. 16 – Table de multiplication du groupe S_3 des permutations de trois objets

Cette table de multiplication nous montre immédiatement que nous pouvons diviser le groupe S_3 par le sous-groupe {I,P,Q} (isomorphe à $\mathbb{Z}_3$), pour obtenir un groupe isomorphe à $\mathbb{Z}_2$.

Nous pouvons voir cela aussi avec les diagrammes de Cayley :

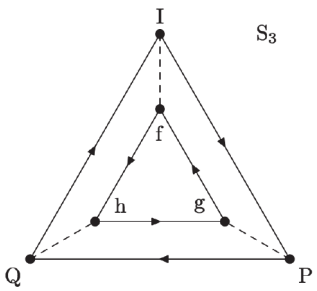


FIG. 17 – Diagramme de Cayley de S_3

La flèche représente la multiplication par P et le pointillé représente la multiplication par f. Nous pouvons *presque* voir sur la figure que {I,P,Q} est un sous-groupe distingué car il est attaché à sa classe latérale par ce que j'ai appelé un *câble* : tous les traits pointillés attachent le sous-groupe à son unique classe latérale[9].
Voici un autre schéma pour éclaircir cette notion de câble :

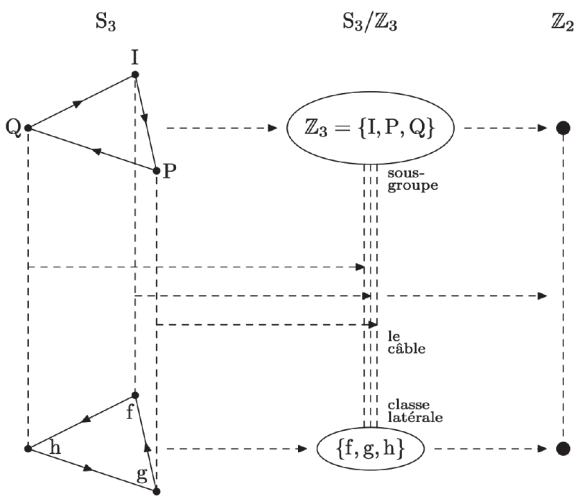


FIG. 18 – Le câble dans S_3

En revanche, si nous considérons le sous-groupe {I,f} :

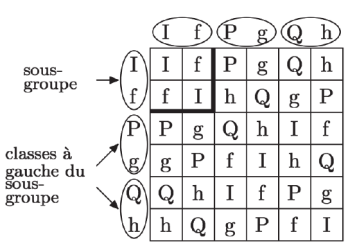


FIG. 19 – Une autre façon de voir la table de multiplication de S_3

(9) C'est un peu banal dans ce cas-ci.

cela se passe moins bien ; il n'est pas possible de diviser S_3 par {I,f}.

Nous pouvons voir cela aussi dans les diagrammes de Cayley :

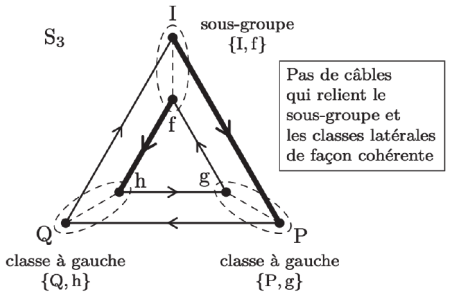


FIG. 20 – Diagramme de Cayley montrant que la division de S_3 par {I,f} est impossible

Le sous-groupe {I,f} est entouré d'un pointillé, ainsi que les deux classes latérales à gauche; si nous multiplions I par P, alors nous obtenons P qui est dans la classe latérale {P,g}, mais si nous multiplions f par P, nous obtenons h qui se trouve dans l'autre classe latérale ; il n'y a donc pas de câble qui relie {I,f} à l'une des classes latérales.

Essayons maintenant de faire le treillis des sous-groupes de S_3 ; nous allons commencer en considérant les trois sous-groupes isomorphes {I,f}, {I.g} et {I,h} : ce sont trois sous-groupes d'ordre 2, non distingués ; ils sont appelés *sous-groupes conjugués*(10).

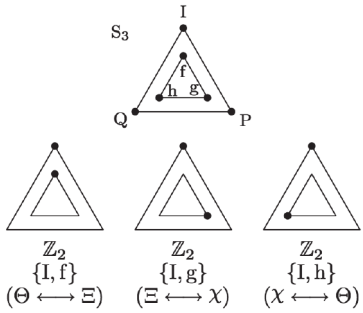


FIG. 21 – S_3 et ses trois sous-groupes conjugués

Nous pouvons alors élaborer le treillis entier des sous-groupes de S_3 (cf. fig.22).

Ce qui est très important, c'est le chemin de droite : en divisant S_3 par {I,P,Q} (isomorphe à $\mathbb{Z}_3$), nous obtenons un groupe isomorphe à $\mathbb{Z}_2$; puis, en divisant (trivialement) {I,P,Q} par {I} (isomorphe à $\mathbb{Z}_1$), nous obtenons un groupe isomorphe à $\mathbb{Z}_3$.

Par le chemin de gauche, en revanche, nous nous retrouvons bloqués, car nous ne pouvons pas diviser S_3 par un de ses sous-groupes conjugués (lignes pointillées).

(10) Ce qui n'est guère surprenant…

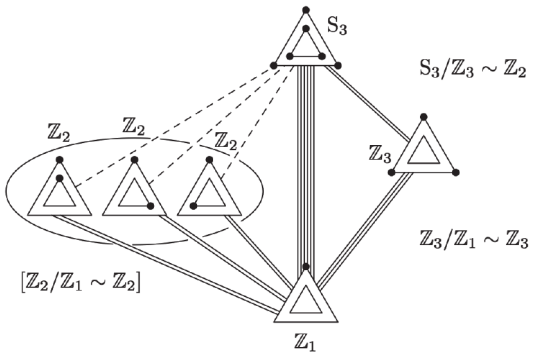


FIG. 22 – Le treillis des sous-groupes de S_3

Comparons maintenant les deux treillis :

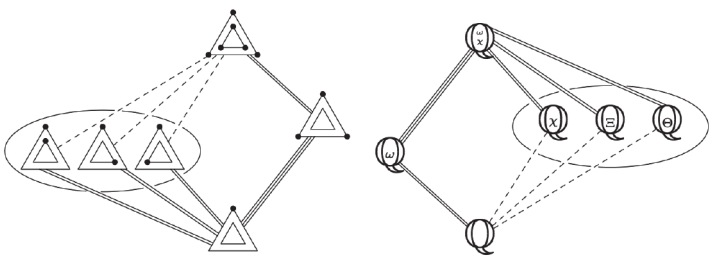


FIG. 23 – Les deux treillis : les sous-groupes de S_3 et les extensions de $\mathbb{Q}$

Nous nous apercevons que ces deux treillis sont (à condition de tourner l'un d'eux de 180°) absolument identiques (isomorphes) et c'est cela la découverte absolument étonnante de Galois, alors qu'il avait environ 17 ou 18 ans…

Voilà un diagramme « *ambigrammatical* » qui combine les deux diagrammes de treillis :

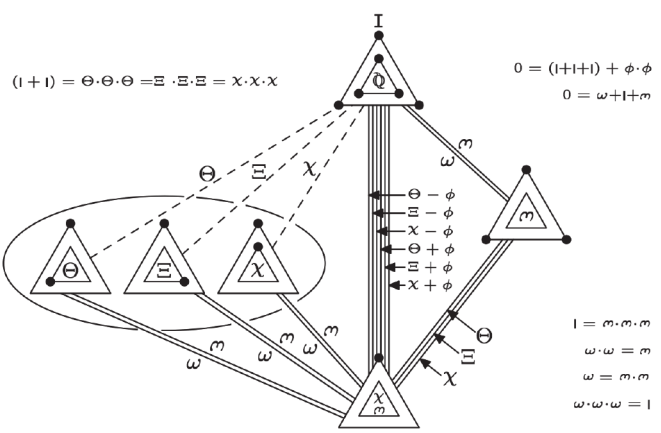


FIG. 24 – Diagramme « *ambigrammatical* » des deux treillis

Ce diagramme peut se lire à l'endroit ou en le tournant de 180°.

En quelque sorte, il y a donc une seule structure, même s'il y a deux treillis d'origines très différentes.

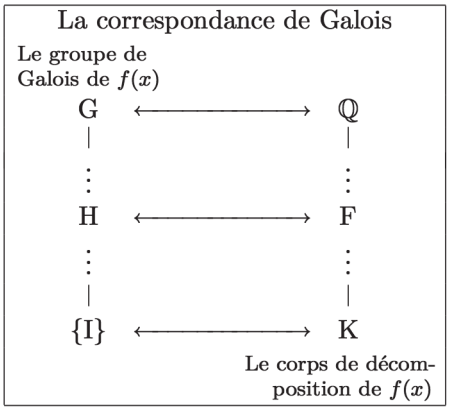
Le théorème fondamental de (la théorie) de Galois

Le *treillis des extensions de corps* entre $\mathbb{Q}$ et le corps de décomposition K d'un polynôme donné $f(x)$ est *isomorphe au treillis des sous-groupes* du groupe G de symétries des racines de $f(x)$ – pourvu que l'un des treillis soit retourné par rapport à l'autre.

Si H est un sous-groupe de G qui correspond au corps intermédiaire F, alors chaque élément de H est une symétrie (un automorphisme) de K qui laisse invariant tous les éléments de F.

Chaque *sous-groupe distingué* correspond à une *extension galoisienne*.

Et chaque famille de *sous-groupes conjugués* correspond à une famille d'*extensions conjuguées*.



Retour aux équations polynomiales

Revenons-en aux équations polynomiales et à la question cruciale de leur résolubilité (ou non!) à l'aide des radicaux.

Découverte de Galois :

À l'ajout du radical[11] $\sqrt[p]{a}$ correspond, dans le treillis des groupes, le groupe cyclique $\mathbb{Z}_p$.

Je ne vais pas démontrer ce théorème mais nous pouvons voir ceci sur un exemple :

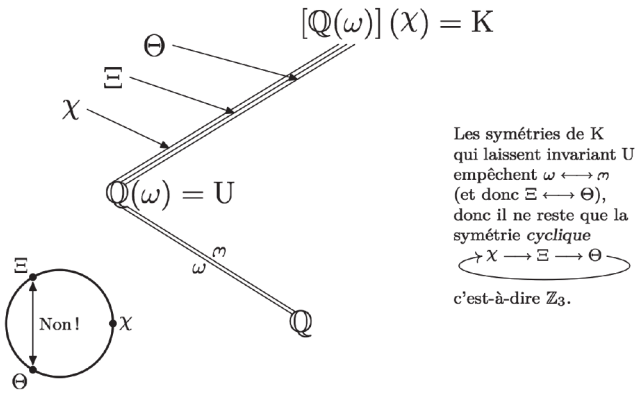


FIG. 25 – La correspondance des groupes cycliques $\mathbb{Z}_p$ aux extensions radicales par $\sqrt[p]{a}$

(11) Ici, p désigne un nombre premier : on montre que l'on peut toujours n'ajouter que des radicaux d'ordre premier.

Lorsque nous passons de U à K et que nous cherchons les automorphismes de K qui laissent U invariant, nous ne pouvons pas échanger Ξ et Θ, car cela reviendrait à échanger ω et $\overline{\omega}$, ce qui est interdit puisque nous voulons fixer U. Il ne nous reste donc comme possibilités que l'identité, la permutation $\chi \to \Xi \to \Theta \to \chi$ et la permutation $\chi \leftarrow \Xi \leftarrow \Theta \leftarrow \chi$, c'est-à-dire $\mathbb{Z}_3$.
Nous commençons donc à percevoir pourquoi les groupes cycliques sont cruciaux.

Généralisation clé :

Une extension radicale

$$\mathrm{U} \to \mathrm{K} = \mathrm{U}\left(\sqrt[p]{a}\right) \quad (a \in U)$$

correspond au groupe de symétries $\mathbb{Z}_p$.
Et, lorsque nous passons du treillis des corps au treillis des groupes, cela se traduit par :

Traduction clé au treillis isomorphe :

Dans le treillis des sous-groupes, $\mathbb{Z}_p$ est le groupe quotient des deux sous-groupes qui correspondent à U et à K.
ce qui peut être représenté par le schéma suivant :

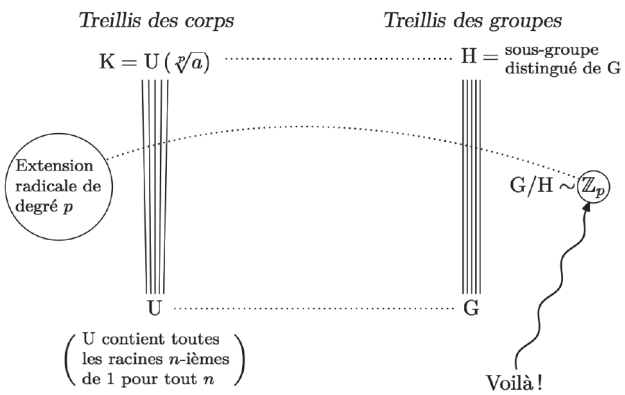


FIG. 26 – Le signe révélateur d'une extension radicale

Le secret galoisien de la résolubilité d'une équation

Une équation polynomiale résoluble à l'aide de racines de divers degrés correspond à un groupe G de symétries qui possède *une chaîne descendante*, depuis G jusqu'à {I}, de *sous-groupes distingués* l'un dans l'autre, et *dont les groupes quotient ont tous la forme* $\mathbb{Z}_p$.
Voici un exemple d'un groupe résoluble à 30 éléments (cf. fig. 27)

En haut (dans G), nous voyons qu'il y a une espèce de structure triadique : si nous divisons G par le sous-groupe G′ (autrement dit, si nous plissons les yeux et que nous regardons uniquement les gros grains, alors nous voyons qu'il y a un diagramme de Cayley qui correspond à $\mathbb{Z}_3$), le groupe quotient est $\mathbb{Z}_3$; dans G′, si nous plissons les

yeux une nouvelle fois, nous apercevons une structure à gros grains qui correspond à $\mathbb{Z}_2$ ($G'/G'' \sim \mathbb{Z}_2$) ; enfin, il est trivial de dire que nous pouvons diviser G'' par son sous-groupe {I} pour obtenir $\mathbb{Z}_5$.

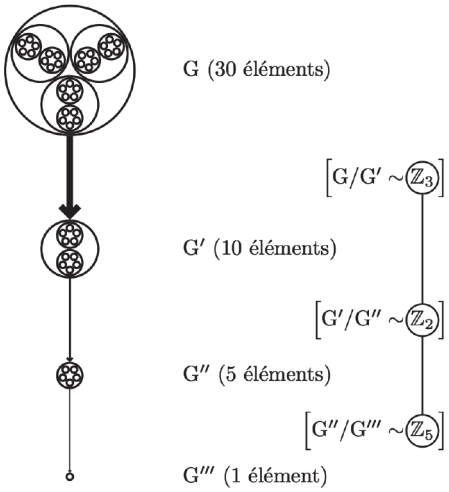


FIG. 27 – Exemple d'un groupe résoluble

Nous obtenons donc une chaîne *descendante* $\mathbb{Z}_3$, $\mathbb{Z}_2$, $\mathbb{Z}_5$, ce qui signifie que le groupe G est *résoluble*.

Équation quartique générale

Nous avions considéré au début une équation quartique dégénérée ($x^4 - x^2 - 2 = 0$) ; que se passe-t-il dans le cas général ?
Pour l'équation *quartique* la plus générale, il y a symétrie totale des 4 racines. Il s'agit donc du groupe S_4 à 24 éléments – le groupe des symétries d'un cube (les 4 diagonales sont permutées de toutes les façons possibles) :

– Un des sous-groupes de S_4 est A_4 (groupe alterné) qui est un sous-groupe distingué de S_4 et qui contient 12 éléments ; en divisant S_4 par A_4, le groupe quotient est donc $\mathbb{Z}_2$;
– A_4 a un sous-groupe distingué (isomorphe au groupe de Klein) de quatre éléments : en divisant A_4 par ce sous-groupe, le groupe quotient est donc $\mathbb{Z}_3$;
– Ensuite, nous avons déjà vu que nous pouvons diviser le groupe de Klein par un sous-groupe distingué à deux éléments (isomorphe à $\mathbb{Z}_2$), ce qui nous donne un groupe quotient $\mathbb{Z}_2$;
– Enfin, le dernier quotient est celui de $\mathbb{Z}_2$ par $\mathbb{Z}_1$, ce qui nous donne encore une fois le groupe quotient $\mathbb{Z}_2$.

La colonne de droite dans la figure 28 est la chaîne descendante des groupes quotient de S_4 jusqu'à $\mathbb{Z}_1$; nous obtenons donc une séquence de groupes cycliques d'ordre premier ($\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_2$, $\mathbb{Z}_2$), ce qui signifie que le groupe S_4 est **résoluble**, ou encore que **l'équation quartique est résoluble par radicaux**.

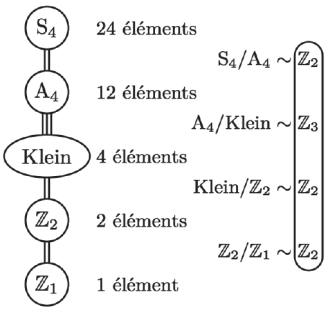


FIG. 28 – Chaîne descendante de S_4 à $\mathbb{Z}_1$

Je ne vais pas vous montrer la solution exacte, mais la forme de la solution est « *une racine quadratique d'une racine quadratique d'une racine cubique d'une racine quadratique* » et ceci correspond exactement, dans l'ordre, aux groupes quotient, comme le montre le schéma suivant :

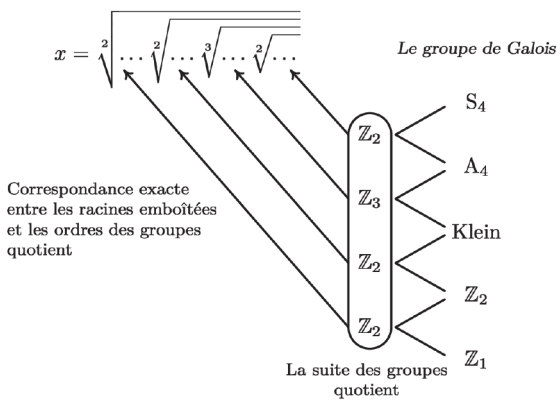


FIG. 29 – Formule de résolution de la quartique générale

Et l'équation quintique ?

Pour l'équation *quintique* la plus générale, il y a symétrie totale des cinq racines – donc S_5 avec $120 = 5!$ éléments.

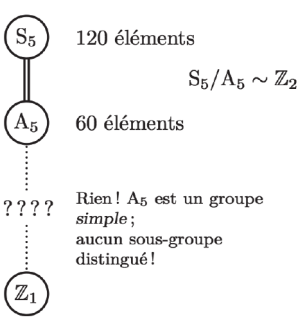


FIG. 30 – Cas de l'équation quintique générale

C'est le groupe des symétries de l'icosaèdre (rotations et réflexions).

– Un des sous-groupes de S_5 est A_5 (groupe alterné) qui est un sous-groupe distingué de S_5 et qui contient 60 éléments; en divisant S_5 par A_5, le groupe quotient est donc $\mathbb{Z}_2$; cela commence bien…

Mais malheureusement, c'est là que l'histoire s'arrête : en effet, A_5 n'a pas de sous-groupe distingué (autre que le sous-groupe trivial $\mathbb{Z}_1$). A_5 est le premier de tous les groupes simples (mis à part les groupes cycliques d'ordre premier comme $\mathbb{Z}_{17}$).
S_5 est donc un groupe **non résoluble**, ce qui signifie que l'équation quintique est **non résoluble par radicaux** !

Conclusion

Nous voyons donc que les clés les plus simples n'ouvrent pas toutes les portes. C'est ça, l'apport de Galois ?

Mais non !

Les idées d'Évariste Galois vont très très loin au-delà de la non résolubilité des équations polynomiales.
– La théorie des groupes abstraits,
– la théorie des corps,
– la théorie des treillis des structures abstraites et de leurs sous-structures,
– la théorie des correspondances entre les treillis,
c'est cela, la « théorie de Galois »

Et les mathématiciens modernes, inspirés par Galois, ont généralisé toutes ces idées à maintes reprises, trouvant partout groupes, treillis, et isomorphies cachées.

Voilà le vrai apport d'Évariste Galois, 180 ans plus tard.

Quel radical !

Et pour le saluer, voilà un portrait de lui[12] :

FIG. 31 – Portrait d'Évariste Galois

Je vous remercie de votre attention.

(12) Il a l'air d'avoir douze ans.