LA PENSÉE D'ÉVARISTE GALOIS ET LE FORMALISME MODERNE

1. Introduction

Il est difficile de dater avec précision le début de l'engagement politique de Galois mais la gravure suivante qui montre, durant la courte révolution de Juillet 1830, les polytechniciens en train de faire le mur pour rejoindre les barricades donne un bon point de départ.

En cette période cruciale (les trois Glorieuses) qui voit la transition de Charles X à Louis-Philippe après la publication des ordonnances le 25 Juillet[1], Galois est Normalien (bien contre son gré après ses deux échecs à Polytechnique) et comme les autres Normaliens est consigné à l'École. Il essaie en vain de faire le mur dans la nuit du 28 au 29 Juillet et nourrit dés lors une rancune tenace contre le directeur du moment, un certain Guigniault que la postérité a généreusement oublié et qui retourne rapidement sa veste à l'arrivée de Louis-Philippe.

28 juillet 1830, les élèves de l'Ecole Polytechnique « font le mur » (Musée Carnavalet).

[1]La première suspend la liberté de la presse ; la seconde dissout la Chambre des députés ; les troisième et quatrième modifient le régime des élections pour assurer une majorité favorable au roi.

Il régnait alors à l'École une discipline bien peu laïque : deux mois sans confession entraînaient un renvoi pur et simple.
Galois n'éprouvait sûrement pas de sympathie pour l'Église, son père s'était suicidé un an avant, victime des attaques d'un curé qui n'hésita pas à faire attribuer à Galois (père) des lettres anonymes qu'il écrivait lui-même. La mise en terre du père Galois, à Bourg La Reine, verra ce curé bousculé par le bon peuple dans une échauffourée. Agonisant après son duel fatal fin Mai 1832, Galois refusera les sacrements d'un prêtre.
En Octobre 1830, Galois entre à L'École Normale pour la deuxième année mais est déjà profondément engagé en politique comme républicain, parti qui se situe bien à gauche des libéraux. Il défend avec verve le droit des masses devant sa famille horrifiée, et s'inscrit en Novembre à la Société des Amis du Peuple parti révolutionnaire d'esprit convention dont la devise est "Progrès social et bien public". Mais ce parti trop idéaliste n'est pas en mesure de compter vraiment en politique et est de plus infiltré par la police.
L'illusion que les choses pouvaient vraiment changer sous Louis-Philippe sera de courte durée. A l'École Normale Galois milite et le milieu de bourgeoisie arriviste des élèves de l'époque ne s'y prête guère ; il est le seul Normalien à faire partie de la Société des Amis du Peuple, les autres élèves tiennent trop à leur carrière. Isolé parmi ses condisciples, critique virulent de l'enseignement prodigué à l'école, Galois est puni de consigne indéfinie ce qui l'empêche de rejoindre les réunions des Amis du Peuple. Il prend alors une grave décision, celle de rendre le conflit public en publiant dans une revue acquise aux républicains (esprit 1793) La gazette des écoles une lettre qui tourne en dérision l'attitude du directeur.
La lettre est signée "Un Élève de l'ENS" mais personne n'est dupe, elle paraît le 5 décembre, le 9 Galois est renvoyé à titre provisoire de L'ENS. Son renvoi sera signé en janvier par Guigniault et Victor Cousin, avec comme l'un des arguments : élève paresseux !
Ceci alors que Galois, à l'âge de 19 ans, a déjà à son actif des résultats mathématiques d'une portée incomparable qui sont l'acte de naissance des mathématiques contemporaines (évitons le mot "moderne" si galvaudé).
Privé de subsistance par son renvoi Galois professe avec succès un "cours d'algèbre" avec une trentaine d'auditeurs dans une petite librairie prés de la Sorbonne. Mais après avoir été acquitté par un jury populaire dans un premier procès, pour avoir levé, un poignard à la main, son verre à la santé de Louis-Philippe, il est arrêté à la tête d'une manifestation et passe la majeure partie de la dernière année de sa vie à la prison Sainte Pélagie dont l'atmosphère de bruyante beuverie bien peu propice au travail intellectuel est décrite par Nerval qui y croisera Galois. De santé fragile Galois sort de prison en Mars 1832, il meurt en duel deux mois plus tard.
Le récit des pertes et refus successifs de ses manuscrits est trop connu pour que l'on s'y attarde ; il suffit sans-doute de mentionner que Galois écrit simplement "Oh, chérubins" sous les arguments des referees qui refusent son article peu avant son deuxième séjour en prison (l'un des referees était pourtant un mathématicien exceptionnel ; il s'agissait de Poisson).
Cette suite tragique de rendez-vous manqués entre Galois et les mathématiciens de son époque (hormis bien sûr ce lien si fort avec Abel, relevant presque de la métempsychose) est merveilleusement interrompue 11 ans après sa mort par la clairvoyance de Liouville en 1843.

Depuis lors l'influence de ses idées n'a jamais faibli, de Sophus Lie à Grothendieck en passant par Émile Picard, la pensée de Galois se reflète indéfiniment chez les mathématiciens et brille, hors du temps, d'un éclat et d'une vigueur difficiles à égaler.
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 fraîcheur nécessaire, *i.e.* en essayant de réfléchir directement aux énoncés sans utiliser l'artillerie lourde.
L'un des aspects des idées de Galois qui est passé le plus facilement dans les outils conceptuels des scientifiques de notre époque est celui relié à la notion de symétrie. Grâce à cet acquis il n'est pas irréaliste d'espérer que les textes de Galois soient devenus accessibles au scientifique non-mathématicien (physicien chimiste et peut-être biologiste). Raison de plus pour en commencer la lecture !

Je remercie J-P. Serre pour ses critiques et corrections, André Dalmas qui m'a fait parvenir la dernière édition de son livre sur Galois [9], J-P. Bourguignon qui m'a signalé le texte de Sophus Lie [19] et Martin Andler qui en me donnant carte blanche pour une lecture d'un texte original me permet de lire avec vous les textes fondateurs de Galois.

2. Brisure de symétrie

Le premier pas de la démarche de Galois consiste à briser de manière maximale la symétrie entre les racines d'une équation en choisissant une fonction auxiliaire largement arbitraire de n variables. Il énonce

Lemme
Étant donnée une équation quelconque, qui n'a pas de racines égales, dont les racines sont a, b, c, $\cdots$, on peut toujours former une fonction V des racines, telle qu'aucune des valeurs que l'on obtient en permutant dans cette fonction les racines de toutes manières ne soient égales.
Preuve
Par exemple on peut prendre

$$V = A\,a + B\,b + C\,c + \cdots$$

où $A, B, C, \cdots$ sont des nombres entiers convenablement choisis.
(On peut même si l'on veut prendre $A = 1$, $B = N$, $C = N^2 \cdots$ avec $N \in \mathbb{N}$ car l'égalité entre deux permutées de V est alors une équation polynomiale en N et n'a qu'un nombre fini de solutions $N \in \mathbb{C}$)

Il en déduit chacune des racines de l'équation de départ comme fonction rationnelle de V :

Lemme
La fonction V étant choisie comme il est indiqué dans l'article précédent, elle jouira de cette propriété que toutes les racines de l'équation proposée s'exprimeront rationnellement en fonction de V.

Preuve Le polynôme suivant en Y a comme coefficients des polynômes en a à coefficients rationnels ,

$$F(Y,a) = \prod_{\sigma}(Y - V(a,\sigma(b),\ldots,\sigma(z)))$$

$$= \sum c_k(a)\, Y^k\,.$$

où σ parcourt l'ensemble des permutations de $(b,c,\cdots,z)$. De plus, avec $\xi = V(a,b,c,\cdots)$, a est la seule racine commune des équations

$$P(X) = 0\,, \quad \sum c_k(X)\,\xi^k = 0\,.$$

d'où $a = f(\xi)$ par élimination euclidienne.

Bien sur, on obtient de même $b = f_2(\xi)$ etc.. Le pas suivant consiste à montrer que remplacer ξ par une autre racine de l'équation en V donne une permutation des racines $a,b,c,\cdots$. Il énonce :

Lemme
Supposons que l'on ait formé l'équation en V, et que l'on ait pris l'un de ses facteurs irréductibles, en sorte que V soit racine d'une équation irréductible. Soient $V, V', V", \cdots$ les racines de cette équation irréductible. Si $a = f(V)$ est une des racines de la proposée, $f(V')$ de même sera une racine de la proposée.

Preuve Si $V = V(a,b,c,\cdots) = \xi$, alors $V' = V(\pi(a),\pi(b),\cdots)$ pour une permutation π, d'où, avec $\pi(a) = b$ on a

$$P(b) = 0\,, F(V',b) = 0$$

ce qui implique

$$b = f(V')\,.$$

Galois note que l'équation $Q(V) = 0$ obtenue à partir d'un facteur irréductible de l'équation en V a cette propriété particulière que ses racines sont fonctions rationnelles de l'une quelconque d'entre elles. En particulier il suffit d'adjoindre formellement une racine de cette équation, en travaillant avec l'algèbre des polynômes modulo les multiples de Q pour adjoindre en fait toutes les racines. Chacune d'entre elles est de la forme $R(x)$ où R est une fonction rationnelle et (toujours en travaillant modulo Q) ces fonctions forment un groupe pour la composition (*i.e.* $R \circ S(x) = R(S(x))$). Ce qui est loin d'être évident à ce stade est que ce groupe est en fait indépendant du choix de la fonction auxiliaire $V(a,b,\cdots,z)$ et ne dépend donc que de l'équation proposée.

3. Groupe de Galois

Le premier point vraiment crucial est la caractérisation conceptuelle du Groupe de Galois qu'il donne sous la forme suivante,

Théorème
Soit une équation donnée, dont a, b, c, $\cdots$ sont les m racines. Il y aura toujours un groupe de permutations des lettres a, b, c, $\cdots$ qui jouira de la propriété suivante :
- 1° que toute fonction des racines, invariable par les substitutions de ce groupe, soit rationnellement connue.
- 2° réciproquement, que toute fonction des racines, déterminable rationnellement, soit invariable par ces substitutions.

Preuve

Les racines de l'équation donnée sont

$$a = f_1(V),\ b = f_2(V), \cdots, z = f_m(V)$$

Le groupe G est formé des permutations

$$\begin{aligned} &f_1(V), f_2(V), \cdots, f_m(V)\\ &f_1(V'), f_2(V'), \cdots, f_m(V')\\ &\cdots\\ &f_1(V^{(d-1)}), f_2(V^{(d-1)}), \cdots, f_m(V^{(d-1)}) \end{aligned}$$

où $V, V', V", \cdots$ sont les racines d'un facteur irréductible Q du polynôme

$$A(Y) = \prod_{\sigma}(Y - V(\sigma(a), \sigma(b), \ldots, \sigma(z)))$$

Il résulte en particulier de la caractérisation donnée par Galois que le groupe G ne dépend pas du choix de la fonction auxiliaire largement arbitraire

$$V(a, b, c, \cdots)$$

que l'on avait choisie pour le construire !

Sa définition demande de manière cruciale de préciser ce que signifie "rationnellement connue" ce que Galois fait en ces termes

"Quand nous disons qu'une fonction est rationnellement connue nous voulons dire que sa valeur numérique est exprimable en fonction rationnelle des coefficients de l'équation et des quantités adjointes

L'ensemble des quantités rationnellement connues forme un *corps* K.
Fixer ce corps K est déterminant dans la décomposition de $A(Y)$ en facteurs irréductibles et donc dans la détermination du groupe de Galois.
En pratique les calculs sont très difficiles à faire mais Galois indique la voie :

"Sauter à pieds joints sur les calculs, grouper les opérations, les classer suivant leurs difficultés et non suivant leur forme, telle est suivant moi, la mission des géomètres futurs"

On dispose d'outils efficaces pour calculer explicitement le groupe de Galois G d'une équation $P(X) = 0$ de degré[2] m

$$P(X) = X^m + a_1 X^{m-1} + \cdots + a_m\,, \quad a_j \in \mathbb{Z}$$

sans avoir à effectuer la décomposition de $A(Y)$ en facteurs irréductibles. Un exemple d'un tel outil est le théorème dû à Dedekind qui assure l'existence dans G d'une permutation ayant des cycles de longueur m_j (où la somme des m_j est le degré m de l'équation) dès que P se factorise, modulo un nombre premier p, en produit de polynômes irréductibles de degré m_j. (On doit choisir p de telle sorte que P n'admette pas de racines multiples modulo p).

C'est en fait Galois qui dans un court article "Sur la théorie des nombres" (Bulletin des sciences Mathématiques 1830) introduit les corps finis les plus généraux

$$\mathbb{F}_q$$

pour $q = p^\ell$. (Le cas $\ell = 1$ est dû à Gauss).
Il démontre que pour construire $\mathbb{F}_q$ il suffit d'adjoindre à $\mathbb{F}_p$ les racines de l'unité d'ordre premier à p, solutions de

$$X^q - X = 0$$

et que toute équation polynomiale sur $\mathbb{F}_p$ se résout complètement dans un $\mathbb{F}_q$.
Il calcule le groupe de Galois de $\mathbb{F}_q$ sur $\mathbb{F}_p$: groupe cyclique engendré par le Frobenius

$$x \to x^p$$

4. Réduction du groupe de Galois

Résoudre une équation c'est décomposer graduellement, par l'adjonction des racines d'équations auxiliaires, son groupe de Galois. Celui-ci énonce :

Théorème
Si l'on adjoint à une équation donnée la racine r d'une équation auxiliaire irréductible,
- 1° il arrivera de deux choses l'une : ou bien le groupe de l'équation ne sera pas changé ; ou bien il se partagera en p groupes appartenant chacun à l'équation proposée respectivement quand on lui adjoint chacune des racines de l'équation auxiliaire ;
- 2° ces groupes jouiront de la propriété remarquable, que l'on passera de l'un à l'autre en opérant dans toutes les permutations du premier une même substitution de lettres.

Ces opérations se traduisent en termes de manipulations sur les groupes et des rudiments de traduction sont donnés dans le tableau suivant.

[2] les programmes actuels permettent d'aller jusqu'à m de l'ordre de 10

Equation $P(X)=0$ **de racines** $a,b,c,\cdots$	**Corps** $K\supset k$ $K=k(a,b,c,\cdots)$	**Groupe de Galois** G=**Gal**(K/k)
Adjonction à k **d'une racine** α**,** $P_1(\alpha)=0$	**Sous-corps** $K_1=k(\alpha)\subset K$	**Sous-groupe** $H_1=\{g\in G\,|\,g\,x=x,\forall x\in K_1\}$
Adjonction à k **de toutes les racines de** P_1	**Extension Normale**	**Sous-groupe Normal**
Equation résoluble par radicaux	$K_j=k(x_1,\cdots,x_j)$ $x_j^{n_j}\in K_{j-1}$	**Groupe résoluble** $G\rhd G_1\rhd\cdots$
Construction à la règle et au compas	**Nombres constructibles**	**Ordre de** $G=2^n$

On notera que H_1 est le groupe de Galois $\mathrm{Gal}(K/K_1)$ de l'extension de K_1 par K. De plus quand K_1 est normal on a $\mathrm{Gal}(K_1/k)=G/H_1$. L'existence d'un sous-groupe normal $H_1\lhd G$ permet de décomposer l'adjonction de toutes les racines de $P(X)=0$ en deux étapes. Dans la première l'on passe de k à K_1 et le groupe de Galois est G/H_1, dans la deuxième on passe de K_1 à K et le groupe de Galois est H_1. Pour illustrer ce mécanisme prenons un exemple.

Les nombres constructibles à la règle et au compas forment un corps. La traduction en termes de groupes de Galois de la fameuse construction (obtenue par Gauss à l'age de 18 ans) à la règle et au compas du polygone régulier à 17 cotés se comprend simplement. L'équation de départ

$$X^{17}-1=0\,,X\neq 1\,,\quad i.e.\ \sum_0^{16}X^k=0$$

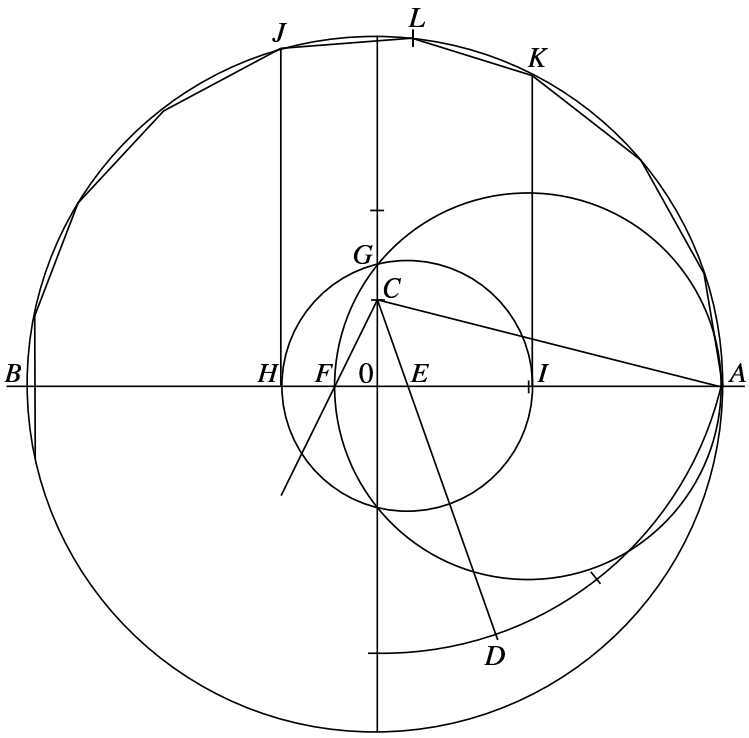
admet pour groupe de Galois le groupe

$$G=\mathbb{F}_{17}^*=\mathbb{Z}/16\,\mathbb{Z}$$

des entiers modulo 16 comme on le voit en notant que ses racines sont fonctions rationnelles de l'une quelconque d'entre elles ce qui permet d'utiliser les fonctions

$$V=a\,,\quad f_n(X)=X^n$$

pour obtenir les substitutions du groupe.



"Tracer deux diamètres perpendiculaires AB et OC où O est le centre et OC le quart du rayon. Tracer AC puis sur le cercle de centre C un arc de A jusqu'au diamètre OC. Prendre le point D aux trois quarts de cet arc. Tracer CD qui coupe AB au point E. Tracer CF à 45 degrés de CE. Prendre le cercle ayant AF pour diamètre. Il intersecte le diamètre OC en un point G. Tracer le cercle de centre E passant par G. Il intersecte la droite AB en H et I. Tracer les perpendiculaires à AB aux points H et I. Elles coupent le grand cercle en J et K. Soit L le milieu de l'arc JK. Alors les points J, K, L, et A sont des sommets du polygone régulier à 17 cotés. Les autres sommets s'en déduisent facilement."

En résolvant le groupe G en quotients successifs l'on suit pas à pas la construction de Gauss. Il est clair que celui-ci, trente ans avant Galois, avait parfaitement compris les principes de la théorie de Galois dans le cas des extensions cyclotomiques. Le groupe de Galois de E est $\mathbb{Z}/4\,\mathbb{Z}$, celui de H (ou de I) est $\mathbb{Z}/8\,\mathbb{Z}$, celui de J (ou K) est $\mathbb{Z}/16\,\mathbb{Z}$.

5. Division des fonctions elliptiques

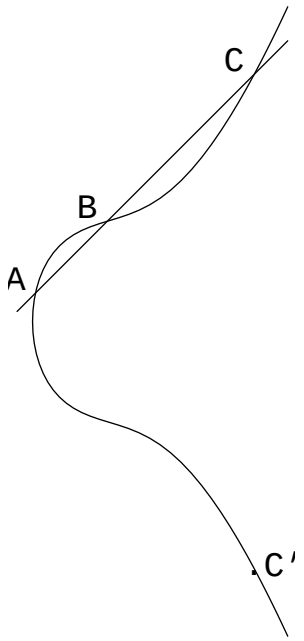
Les formules d'addition en trigonométrie

$$\tan(a+b) = \frac{\tan(a) + \tan(b)}{1 - \tan(a)\tan(b)}$$

définissent une loi de groupe sur $\mathbb{P}_1(\mathbb{R})$ mais la beauté de cette loi

$$(t, t') \to \frac{t + t'}{1 - t\,t'}$$

a ses limites car elle ne donne pas une loi de groupe sur $\mathbb{P}_1(\mathbb{C})$: l'addition de $i = \sqrt{-1}$ est singulière.



$$A + B = C'$$

Seules les courbes de caractéristique d'Euler nulle (*i.e.* de genre 1) peuvent posséder une telle loi de groupe qui ne soit pas singulière dans le domaine complexe .
C'est le cas des courbes elliptiques

$$Y^2 = 4\,X^3 - g_2\,X - g_3\,, \quad \Delta = g_2^3 - 27\,g_3^2 \neq 0$$

qui sont le premier exemple de groupe abélien.

La loi d'addition dans le groupe formé des points complexes de la courbe est la suivante : étant donnés A et B la somme $A + B = C'$ est obtenue en prenant le symétrique par rapport à l'axe des x, axe de symétrie de la courbe, du point d'intersection C de la droite AB avec la courbe. Comme la courbe est de degré 3 le point C est bien défini. Quand $A = B$ on remplace la droite AB par la tangente en A. Les coordonnées de C' dépendent rationnellement de celles de A et de B.
La notion familière de racine N-ième de l'unité devient alors celle de point de N-torsion de la courbe elliptique. De tels points sont solutions de l'équation

$$N \times P = O\,, \quad i.e.\ P + P + P + \cdots + P = O\,,$$

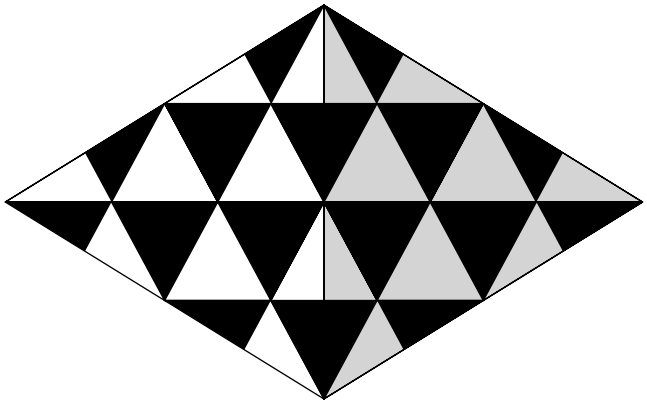
où le point O est l'élément neutre du groupe, qui se trouve être ici un point à l'infini dans le plan projectif complexe $\mathbb{P}_2(\mathbb{C})$.

L'invariant fondamental de la courbe elliptique est

$$j = 1728\,\frac{g_2^3}{\Delta}\,.$$

Les coordonnées X des points de torsion sont (à la normalisation près) solutions d'équations à coefficients dans le corps $\mathbb{Q}(j)$ et la situation dépend de la nature du nombre j. Si j est un nombre transcendant la situation est indépendante de sa valeur numérique et peut en fait se décrire directement en donnant des formules explicites pour les coordonnées des points de torsion.
On commence par trouver un nombre complexe τ de partie imaginaire positive tel que la courbe elliptique soit isomorphe en tant que groupe complexe au quotient du groupe additif de $\mathbb{C}$ par le réseau $L = \mathbb{Z} + \tau\,\mathbb{Z}$. On a alors $j = J(q)$ avec $q = e^{2\pi i\tau}$ où la fonction modulaire J est donnée par une série en puissances de q, qui n'est autre que l'invariant $J = 1728\,\frac{G_2^3}{\Delta}$ où G_2 et G_3 se calculent directement à partir du réseau L (comme somme sur ses éléments non nuls)

$$G_2 = 60\sum\frac{1}{(n+m\,\tau)^4}\,,\quad G_3 = 140\sum\frac{1}{(n+m\,\tau)^6}\,.$$



La série en puissances de q donnant J est à coefficients entiers

$$J(q) = \frac{1}{q} + 744 + 196884\,q + 21493760\,q^2 + \cdots$$

A un facteur de normalisation prés, les coordonnées X des points de torsion de la courbe elliptique sont alors données de la manière suivante : pour $(a,b) \in \{0,1,\ldots,N-1\}^2 \neq (0,0)$, soit

$$E_{a,b}(q) = \frac{1}{12} + \frac{z}{(1-z)^2} + \sum_{n,d|n} d\,(z^d + z^{-d} - 2)\,q^n\,,$$

avec $z = e^{2\pi i\frac{a}{N}}\,q^{\frac{-b}{N}}$. Posons

$$f_{a,b}(q) = \frac{G_2\,G_3}{\Delta}\,E_{a,b}(q)\,.$$

Tous les coefficients de la série en puissances de q sont dans $\mathbb{Q}\,[e^{2\pi i/N}]$.

Le corps F_N engendré par les $f_{a,b}$ est une extension algébrique finie Galoisienne de $\mathbb{Q}(j)$ de groupe de Galois

$$\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\pm 1$$

agissant par permutations des indices (a, b). Le corps $F = \cup F_N$ est une extension transcendante de $\mathbb{Q}$ dont le groupe de Galois a été calculé par Shimura.

Tous ces énoncés sont valables quand le nombre j est transcendant. Il n'en est plus de même quand j est un nombre algébrique et, dans ce cas là, la situation est très différente selon que la courbe elliptique est ou non à multiplication complexe, notion découverte par Abel, qui signifie qu'il existe un nombre complexe $\mu \notin \mathbb{Z}$ tel que $\mu\, L \subset L$ (calculer μ dans l'exemple du réseau équilatéral de la figure ci-dessus). Cette situation se produit quand le nombre complexe τ est de la forme $\tau = \sqrt{-D}$ où D est un entier positif qui n'est pas un carré. Dans ce cas là, un résultat dû à Kronecker, le fameux Jugendtraum, montre que les coordonnées X des points de torsion de la courbe elliptique[3] engendrent l'extension abélienne maximale (*i.e.* la réunion de toutes les extensions normales de groupe de Galois abélien) du corps quadratique imaginaire $K = \mathbb{Q}(\sqrt{-D}\,)$.
Dans le cas où la courbe elliptique, définie sur $\bar{\mathbb{Q}}$, n'est pas à multiplication complexe un résultat de Serre ([25]) montre que la situation est radicalement différente et que par exemple pour p premier assez grand le groupe de Galois des points de p-torsion de la courbe est égal à $\mathrm{GL}_2(\mathbb{F}_p)$.

[3]en fait le produit $\frac{g_2\, g_3}{\Delta} \times X$ en supposant $g_j \neq 0$

6. La lettre testament

Dans sa lettre testament à son ami Auguste Chevalier, datée du 29 Mai 1832, la veille du duel fatal, Galois explique comment sa théorie s'applique à l'extension par les points de division des courbes elliptiques, il sait qu'elle est normale et que son groupe de Galois est contenu dans $\mathrm{GL}_2/\pm$,

"On sait que le groupe de l'équation qui a pour racines les sinus de l'amplitude des p^2-1 divisions d'une période est celui-ci

$$x_{k/\ell} \quad x_{ak+b\ell/\,ck+d\ell}\ "$$

Les sinus de l'amplitude sont les coordonnées x dans les notations de Jacobi, on a $x = \mathrm{sn}(u,k) = \sin(\mathrm{am}(u,k))$ et l'équation de la courbe est $y^2 = (1-x^2)(1-k^2\,x^2)$.

Dans le troisième mémoire annoncé dans cette lettre, Galois en s'appuyant sur le dernier mémoire d'Abel anticipe les résultats essentiels de la théorie des intégrales abéliennes que Riemann obtiendra 25 ans plus tard. Citons Jean Dieudonné,

"Il est certes superflu de redire après tant d'autres ce que la mathématique doit à Galois. Chacun sait que ses idées sont à la source même de l'Algèbre moderne ; ce qui est peut-être moins connu, c'est qu'il était aussi, sans doute possible, parvenu à l'essentiel de la théorie des intégrales abéliennes, telle que Riemann devait la développer 25 ans plus tard"

Avant de terminer cet essai sur une rapide évocation de développements actuels qui se situent directement dans la dynamique des idées de Galois il convient de citer la fin de sa lettre testament.

"Tu sais, mon cher Auguste, que ces sujets ne sont pas les seuls que j'aie explorés. Mes principales méditations depuis quelque temps étaient dirigées sur l'application à l'analyse transcendante de la théorie de l'ambiguïté. Il s'agissait de voir a priori dans une relation entre des quantités ou fonctions transcendantes quels échanges on pouvait faire, quelles quantités on pouvait substituer aux quantités données sans que la relation pût cesser d'avoir lieu. Cela fait reconnaitre tout de suite l'impossibilité de beaucoup d'expressions que l'on pourrait chercher. Mais je n'ai pas le temps et mes idées ne sont pas encore assez développées sur ce terrain qui est immense"

7. Développements Actuels

Loin d'être passées de mode les idées de Galois irriguent encore les mathématiques contemporaines. J'en donnerai un bref aperçu ci-dessous, qui bien entendu est loin d'être exhaustif et ne reflète que le biais de mes intérêts actuels.

7.1. **Motifs.**

La théorie des motifs due à Grothendieck est une généralisation naturelle de la théorie de Galois en dimension > 0 *i.e.* si l'on veut aux polynômes à plusieurs variables. C'est à Weil que l'on doit d'avoir compris que le groupe des points de torsion d'une courbe elliptique (et plus généralement des points de torsion de la Jacobienne d'une courbe) était en fait le reflet d'une théorie cohomologique. Le module de Tate formé comme la limite projective des groupes de torsion (d'ordre une puissance d'un nombre premier ℓ) porte une représentation naturelle du groupe de Galois absolu et cette action de Galois sur la cohomologie est un invariant fondamental.
La théorie cohomologique en question n'a pris sa forme actuelle que dans la cohomologie étale ℓ-adique dont la gestation est merveilleusement visible dans la correspondance Grothendieck-Serre ([6]). La nécessité de comparer entre elles ces théories pour différents choix du nombre premier ℓ et la présence d'autres cohomologies telles celle de de Rham (qui est purement algébrique grâce aux résultats fondamentaux de Serre) et de Betti (qui implique un plongement du corps de définition dans $\mathbb{C}$) ont conduit Grothendieck à dégager le motif commun à tous ces avatars cohomologiques.
Sous sa forme la plus simple la théorie des motifs purs consiste à linéariser la catégorie des variétés projectives lisses sur un corps k. Les morphismes sont les correspondances algébriques modulo l'équivalence numérique (qui ne retient que les nombres d'intersection avec les sous-variétés de dimension complémentaire). La linéarisation requiert de rajouter de nouveaux objets, images de morphismes égaux à leur carré ($e^2 = e$). L'on obtient alors une catégorie abélienne semi-simple[4], la catégorie des *motifs numériques effectifs* et un foncteur naturel H qui associe à toute variété son motif (la variété elle-même) et joue le rôle de théorie cohomologique universelle.
La sous-catégorie dont les objets proviennent des k-variétés projectives lisses de dimension 0 est équivalente à la catégorie des représentations du groupe de Galois $\mathrm{Gal}(\bar{k}/k)$ dans un $\mathbb{Q}$-espace vectoriel de dimension finie. Pour reconstruire le groupe $\mathrm{Gal}(\bar{k}/k)$ à partir de cette catégorie abélienne il faut la doter de la structure supplémentaire donnée par le produit des variétés du côté géométrique. Cela correspond au produit tensoriel des représentations et permet (en invoquant un foncteur fibre) de retrouver le groupe de Galois $\mathrm{Gal}(\bar{k}/k)$ à partir des motifs numériques de dimension 0. C'est en ce sens que la théorie générale des motifs de dimension arbitraire constitue une vaste généralisation de la théorie de Galois (voir par exemple [1]). Ceci suggère en particulier de définir un groupe de Galois motivique pur en dimension supérieure à partir de la catégorie des motifs numériques dotée de la structure tensorielle provenant du produit des variétés. Cette idée de Grothendieck s'est montrée d'une remarquable fécondité malgré le caractère conjectural de bon nombre d'énoncés.

7.2. **Correspondance de Riemann-Hilbert.**

La théorie de Galois différentielle initiée par Picard et Vessiot et calquée sur les idées de Galois et Lie ([19]) joue, pour les équations différentielles, le même rôle que la

[4]résultat conjecturé par Grothendieck et prouvé par Jannsen en 91

théorie de Galois classique pour les équations algébriques. Elle a été profondément renouvelée au début des années 80 sous l'influence des travaux de Ramis, Sibuya, Martinet et Malgrange ainsi que de ceux d'Ecalle sur la résurgence.
Vers 1900 Schlesinger avait montré que pour une équation différentielle linéaire rationnelle de type Fuchs, *i.e.* à singularités régulières, le groupe de Galois différentiel est l'adhérence de Zariski du sous-groupe de monodromie. Il remarquait aussi que ce résultat n'est plus vrai dans le cas général des singularités irrégulières. En 1985 Ramis a montré comment modifier ce résultat pour qu'il reste valable (pour le groupe de Galois local) dans le cas général. Il faut pour cela ajouter à la monodromie formelle deux groupes le tore exponentiel et le groupe de ramification sauvage qui provient des multiplicateurs de Stokes (exponentielles des dérivations étrangères d'Ecalle). Cela permet la formulation en termes galoisiens de l'ambiguïté inhérente aux procédés de sommation, comme dans le phénomène de Stokes.
Cela a permis à J-P Ramis de développer en profondeur les applications à l'analyse des intuitions de Galois sur la théorie de l'ambiguïté et de montrer par exemple que tout groupe algébrique semi-simple est un groupe de Galois différentiel local. Citons Ramis sur Galois, [24]

"Il est impossible de savoir si Galois avait quelque idée du phénomène de Stokes et de sa nature galoisienne. Par contre je suis certain qu'il avait compris la nature "galoisienne" de certaines transformations en analyse complexe (ambiguïtés) comme le recalibrage des exponentielles (dont le prototype est le remplacement dans toutes les formules de $e^{1/x}$ par $\lambda\, e^{1/x}$, λ étant un nombre complexe non-nul fixé)."

Le tore exponentiel de Ramis code exactement ce recalibrage des exponentielles qui apparaissent dans les solutions formelles. Pour le groupe de ramification sauvage, les difficultés essentielles relèvent de l'analyse des procédés de sommation des séries divergentes mais l'on y gagne beaucoup à tout reformuler en termes de correspondance de Riemann-Hilbert [5].
L'origine de la terminologie vient du problème de Riemann-Hilbert, l'un des fameux problèmes de Hilbert, qui consiste à chercher une équation Fuchsienne de monodromie donnée. Bien que le problème tel qu'il était formulé par Hilbert ait une réponse positive, il faut affiner la notion de singularité régulière pour que la réponse soit positive en général et Deligne en a obtenu une vaste généralisation en dimension arbitraire ([10]).
La théorie des catégories Tannakiennes initiée par Grothendieck à propos des motifs (pour reconstruire le groupe de Galois motivique) et développée par Saavedra puis Deligne ([12]) est une clé qui permet de mieux comprendre ces résultats et dans bien d'autres circonstances de traduire une situation géométrique en termes de représentations de groupes. C'est le cas en particulier pour l'étude des équations différentielles et la correspondance de Riemann-Hilbert permet en particulier de replacer la théorie de Galois différentielle dans la même perspective que celle des motifs. Elle joue également un rôle clé dans le pendant géométrique du programme de Langlands, *i.e.* la transposition de la correspondance de Langlands du cas des corps de fonctions sur un corps fini à celui des corps de fonctions sur $\mathbb{C}$.

[5] appelée "correspondance du Bon Dieu" par Grothendieck dans un moment d'exaspération

7.3. **Dessins d'enfants (**$\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$**).**

Dans l'esquisse d'un programme que Grothendieck écrivit pour présenter sa candidature[6] au CNRS dans les années 80, il exhibe une merveilleuse représentation géométrique du groupe de Galois $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, l'un des objets les plus intéressant des mathématiques. La mise en œuvre de ce programme s'appuie sur des résultats de Belyi, Grothendieck, Shabat et Voevodsky qui permettent (*cf.* [3]) d'énoncer pour une courbe lisse C sur $\mathbb{C}$ l'équivalence des conditions suivantes :

- C peut être définie sur $\bar{\mathbb{Q}}$
- C est la compactification canonique d'un revêtement fini non-ramifié de $\mathbb{P}^1(\mathbb{C})$ dont on a enlevé les trois points $\{0, 1, \infty\}$.
- C est isomorphe à la compactification canonique du quotient du demi-plan de Poincaré par l'action d'un sous-groupe d'indice fini de $\mathrm{PSL}(2, \mathbb{Z})$.
- En tant que variété conforme C est obtenue en recollant entre eux un nombre fini de triangles équilatères (dotés de la structure conforme Euclidienne).

Comme les revêtements finis étales constituent le pendant géométrique du groupe fondamental étale , Grothendieck en déduit une représentation naturelle du groupe de Galois $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ comme automorphismes de

$$G = \pi_1^{\mathrm{etale}}(\mathbb{P}^1(\mathbb{C})\backslash\{0, 1, \infty\})$$

En fait l'objet naturel associé à l'action ci-dessus est la suite exacte de groupes

$$1 \to \pi_1^{\mathrm{etale}}(X_{\bar{\mathbb{Q}}}) \to \pi_1^{\mathrm{etale}}(X_{\mathbb{Q}}) \to \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to 1$$

où X désigne le schéma $\mathbb{P}^1\backslash\{0, 1, \infty\}$ qui correspond simplement à l'algèbre des fractions rationnelles $R(z)$ dont les pôles sont dans $\{0, 1, \infty\}$. Le terme de gauche est inchangé si l'on remplace la clôture algébrique $\bar{\mathbb{Q}}$ de $\mathbb{Q}$ par n'importe quel corps algébriquement clos, de caractéristique nulle, tel $\mathbb{C}$ qui donne bien le groupe G introduit plus haut. Le terme de droite $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ n'est autre que le π_1^{etale} du schéma $\mathrm{Spec}\ \mathbb{Q}$ et l'on voit bien, sur cet exemple, l'intérêt du formalisme des schémas où groupes de Galois et groupes fondamentaux sont traités simultanément.

Dans le contexte des algèbres de quasi-Hopf Drinfel'd [14] a été amené à introduire un groupe de Grothendieck–Teichmüller GT, qui est la version pro-unipotente du groupe des automorphismes du groupe fondamental de $\mathbb{P}^1\backslash\{0, 1, \infty\}$. L'étude motivique de cet objet (*cf.* [13]) est intimement reliée à des questions profondes d'arithmétique comme les relations entre nombres d'Euler-Zagier ([4]). Elle implique les motifs de Tate mixtes (et le groupe de Galois motivique $G_{\mathcal{M}_T}(\mathbb{Z})$ ([13]) du schéma $\mathrm{Spec}(\mathbb{Z})$) que nous retrouverons dans la dernière section ci-dessous.

7.4. **Groupe de Galois Cosmique.**

Dans son article pour les quarante ans de l'IHES, intitulé "La folle journée" ([5]), Pierre Cartier avait exprimé l'espoir d'une synthèse entre les idées de Grothendieck sur les motifs, et la renormalisation en théorie quantique des champs dévissée comme nous l'avions fait dans un travail ([7]) en collaboration avec Dirk Kreimer. La clé de ce travail, après la découverte par Dirk de la structure de Hopf sous-jacente aux graphes de Feynman, était l'identité miraculeuse entre le procédé récursif utilisé par les physiciens (sous le nom de renormalisation) pour éliminer les divergences et

[6] il ne lui fut accordé qu'un poste provisoire qui ne fut obtenu que de haute lutte après avoir déjoué le verrouillage des syndicats !

la décomposition de Birkhoff des lacets à valeurs dans un groupe de Lie complexe. Dans un travail très récent ([8]) en collaboration avec Matilde Marcolli nous venons de réaliser ce rêve de Cartier. Comme celui-ci le suggérait il existe un "groupe de Galois cosmique" U^* qui régit la théorie des champs en physique et contient le groupe de renormalisation comme sous-groupe à un paramètre. Ce groupe de Galois cosmique apparaît grâce à la correspondance de Riemann-Hilbert à partir du problème géométrique de classification des connections plates équisingulières. Le support géométrique B de ces connections est donné par le procédé de régularisation dimensionnelle qui fournit, du fait de l'arbitraire dans la normalisation de l'intégrale en dimension complexe $d = D - z$, un fibré principal B de groupe $\mathbb{G}_m = \mathbb{C}^*$, de base un disque infinitésimal Δ centré en D. La fibre $\pi^{-1}(d)$ du fibré B au-dessus de $d \in \Delta$ est l'ensemble des normalisations possibles de l'intégration en dimension d. La fibre spéciale $V = \pi^{-1}(D)$ joue un rôle particulier à cause des divergences de sorte que la connexion est singulière sur $V \subset B$. Ces singularités ne sont pas régulières et le modèle est la théorie de Ramis dans le cadre formel. La catégorie des fibrés plats équisinguliers est équivalente à la catégorie des représentations de dimension finie d'un (unique) groupe algébrique affine U^*. Ce groupe est le produit semi-direct par $\mathbb{G}_m$ (agissant par la graduation) du groupe pro-unipotent U dont l'algèbre de Lie

$$\mathrm{Lie}(U) = \mathcal{F}(1, 2, 3, \cdots).$$

est librement engendrée par un générateur de degré n pour tout entier $n \geq 1$.
Nous montrons que les divergences de la théorie des champs codent, en fait, exactement l'action de ce *groupe de Galois motivique* explicite sur l'ensemble des théories physiques. Le groupe de renormalisation apparaît comme un sous-groupe à un paramètre $\mathbb{G}_a \subset U^*$ du groupe de Galois U^*.

Nous développons de plus l'analogie entre la catégorie des fibrés plats équisinguliers et celle des motifs de Tate mixtes. (Voir [1] pour la nuance importante entre les motifs purs décrits pus haut et les motifs mixtes). On sait, en particulier, que le groupe de Galois motivique $G_{\mathcal{M}_T}(\mathcal{O})$ ([13]) du schéma $S_4 = \mathrm{Spec}(\mathcal{O})$ associé aux racines quatrièmes de l'unité (de sorte que $\mathcal{O}$ est l'anneau $\mathbb{Z}[i][\frac{1}{2}]$) est (non-canoniquement) isomorphe au groupe U^*.

L'ensemble de ces résultats montre que les divergences de la théorie des champs indiquent, en fait, la présence de symétries de nature galoisienne et, bien loin d'être des imperfections de la physique révèlent à n'en pas douter la subtilité de la géométrie qui gouverne l'espace-temps, une fois prise en compte la régularisation dimensionnelle.

Références

[1] Y. André, *Une introduction aux motifs*, Panoramas et Synthèses **17**, Société Mathématique de France, (2004).

[2] R. Bourgne, D. Azra, *Ecrits et mémoires mathématiques d'Evariste Galois*, Gauthier-Villars, Paris (1962).

[3] J-B. Bost, *Introduction to compact Riemann surfaces, Jacobians, and Abelian Varieties*, From Number Theory to Physics, Springer-Verlag, Berlin (1992).

[4] P. Cartier, *Fonctions polylogarithmes, nombres polyzêtas et groupes pro-unipotents.* Séminaire Bourbaki, Vol. 2000/2001. Astérisque No. 282 (2002), Exp. No. 885, viii, 137–173.

[5] P. Cartier, *A mad day's work : from Grothendieck to Connes and Kontsevich. The evolution of concepts of space and symmetry*, Bull. Amer. Math. Soc. (N.S.) 38 (2001), no. 4, 389–408.

[6] P. Colmez, J-P. Serre *Correspondance Grothendieck-Serre*, Société Mathématique de France, (2001).

[7] A. Connes, D. Kreimer, *Renormalization in quantum field theory and the Riemann-Hilbert problem I : the Hopf algebra structure of graphs and the main theorem*, hep-th/9912092. *Renormalization in quantum field theory and the Riemann-Hilbert problem II : The β function, diffeomorphisms and the renormalization group*, hep-th/0003188.

[8] A. Connes, M. Marcolli, *Renormalization and motivic Galois theory.* International Math. Research Notices, **76** (2004), 4073–4092, Math NT/0409306.

[9] A. Dalmas, *Evariste Galois, Révolutionnaire et Géomètre*, Editions Libelles, Fasquelle (1956).

[10] P. Deligne, *Equations différentielles à points singuliers réguliers*, Lecture Notes in Mathematics 163, Springer 1970.

[11] P. Deligne, *Le groupe fondamental de la droite projective moins trois points*, in "Galois group over $\mathbb{Q}$" MSRI Publications Vol. 16, pp. 79–313, Springer Verlag, 1989.

[12] P. Deligne, *Catégories tannakiennes*, in "Grothendieck Festschrift" Vol.2, pp. 111–195, Progress in Mathematics Vol.87, Birkhäuser, 1990.

[13] P. Deligne, A.B. Goncharov *Groupes fondamentaux motiviques de Tate mixte.* Annales Scientifiques de l'ENS.

[14] V. Drinfel'd, *On quasitriangular quasi-Hopf algebras and on a group that is closely connected with* $\mathrm{Gal}(\overline{Q}/Q)$. Algebra i Analiz 2 (1990), no. 4, 149–181 ; English translation in Leningrad Math. J. 2 (1991), no. 4, 829–860.

[15] J. Ecalle, *Singularités irrégulières et résurgence multiple, Cinq applications des fonctions résurgentes* (preprint 84T 62, Orsay), 2-42.

[16] A. Grothendieck, *Esquisse d'un programme*, (1984), paru dans "Geometric Galois actions, 1", 5–48, Cambridge Univ. Press, 1997.

[17] A. Grothendieck, *Récoltes et semailles.*

[18] M. Kontsevich, D. Zagier, *Periods*, in "Mathematics unlimited—2001 and beyond", pp. 771–808, Springer, 2001.

[19] S. Lie, *Influence de Galois sur le développement des mathématiques*, Centenaire de l'Ecole Normale Supérieure, Paris, Hachette (1895) 481-489. 331–401.

[20] J. Martinet, J.P. Ramis, *Elementary acceleration and multisummability, I*, Ann. Inst. Henri Poincaré, Vol.54 (1991) 331–401.

[21] Z. Mebkhout, *Sur le problème de Hilbert-Riemann* C. R. Acad. Sci. Paris Sér. A-B 290 (1980), no. 9, A415–A417

[22] J. Milne, *Fields and Galois theory*, http ://www.jmilne.org/math/CourseNotes/math594f.pdf

[23] J. Milne, *Lectures on Etale Cohomology*, http ://www.jmilne.org/math/CourseNotes/math732.html

[24] J.P. Ramis, *Séries divergentes et théories asymptotiques.* Bull. Soc. Math. France, 121(Panoramas et Syntheses, suppl.) 74, 1993.

[25] J.P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques.* Inventiones Math. **15**, 1972, 259-331.