wikisource Manuscrits de Galois, édition Tannery 1908, Ecrits mathématiques inédits de Galois

ÉCRITS MATHÉMATIQUES INÉDITS.

En dehors des quelques fragments que l'on trouvera plus loin, les écrits mathématiques de Galois que Liouville n'a pas publiés contiennent une cinquantaine de feuilles détachées ([1]) pleines de calculs qui, pour la plupart, concernent la théorie des fonctions elliptiques et remontent sans doute à un moment où Galois étudiait les Mémoires de Jacobi ([2]), quatre pages sur les équations aux dérivées partielles du premier ordre, quelques calculs, avec un commencement de rédaction, sur les intégrales eulériennes ([3]), huit lignes, dont plusieurs mots sont déchirés, qui paraissent se rapporter au groupe alterné et n'avoir pas grand intérêt, un cahier dont la plupart des pages sont blanches et dont je dirai tout à l'heure deux mots, enfin une vingtaine de lignes sur le théorème d'Abel.

Ces vingt lignes peuvent être regardées comme un résumé de la célèbre "Démonstration d'une propriété générale d'une certaine classe de fonctions transcendantes" ([4]), qui est datée de 1829 ; elles occupent les deux tiers de la première page d'une feuille double de même format (30 x 15) que la lettre à Chevalier. On lit en haut de la page :

Théorie des fonctions de la forme $\int X\,\mathrm{d}x$, X étant une fonction algébrique de x.

Les mots "fonctions de la...", jusqu'à la fin, sont biffés et Galois a écrit au-dessus

intégrales dont les différentielles est algébrique.

Le premier titre est presque identique à ceux qui ont été signalés précédemment (p. 17 et p. 23). dont l'un porte la mention "septembre 1831". L'énoncé du théorème d'Abel (qui n'est pas nommé) est précédé des mots "Lemme fondamental". Après la démonstration on lit

Remarque. Dans le cas où

Le reste de la page, les deux pages qui suivent sont en blanc ([5]). Ces quelques lignes sont-elles tout ce qui reste du troisième *Mémoire qui concerne les intégrales*, que Galois résume dans la lettre à Chevalier ? Ce troisième Mémoire a-t-il été rédigé ? Je rappelle quelques termes de la lettre

On pourra faire avec tout cela trois Mémoires.

Le premier est écrit, et... je le maintiens... . . . tout ce que j'ai écrit là est depuis bientôt un an dans ma tête.

Le premier est écrit semble indiquer que les autres ne sont pas rédigés. *On pourra faire avec tout cela trois Mémoires* porte à penser que Galois laissait des notes, dont on ne peut plus espérer aujourd'hui qu'elles soient retrouvées. Une seule chose est certaine, c'est que, la veille de sa mort, *il avait tout cela dans la tête.*

Le cahier est du format 20 x 15 ; on lit sur la couverture : Notes de mathématiques, quatorze pages, seulement, sont utilisées. On trouve dans ce cahier et, parfois, sur la même page, deux sortes d'écriture : pour l'une, il n'y a pas de doute, c'est bien celle de Galois, avec son allure habituelle. L'autre, beaucoup moins lisible, est droite. Je me suis demandé si Galois ne s'était pas amusé à déformer son écriture ; mais M. Paul Dupuy, après un examen attentif des deux écritures, a constaté qu'elles révélaient des habitudes très différentes : elles ne sont pas de la même personne.

Au reste, ce cahier, par son contenu, n'offre qu'un intérêt médiocre. Les pages qui sont de Galois contiennent quelques remarques sur les asymptotes des courbes algébriques et un court essai sur les principes de l'Analyse, dont je citerai quelques lignes ; elles caractérisent un état d'esprit qui résultait sans doute de l'enseignement que Galois avait reçu ; on n'oubliera pas qu'il n'était sans doute alors qu'un écolier, un écolier qui, peut-être, avait approfondi déjà des problèmes singulièrement difficiles.

Après avoir expliqué comment il juge la méthode de Lagrange, où le développement de Taylor tient le rôle essentiel, préférable à la méthode qui consiste à partir de la notion de dérivée considérée comme la limité de l'expression

$$\frac{f(X)-f(x)}{X-x},$$

limite qui ne peut être constamment nulle ou infinie, et comment le raisonnement de Lagrange ne tient pas debout, il propose de lui substituer le suivant :

Considérons d'abord une fonction $\phi(z)$ qui devienne nulle pour la valeur 0 de la variable. Je dis que l'on pourra toujours déterminer un seul nombre positif et fini n de manière que $\frac{\phi(z)}{z^n}$ ne soit ni nulle ni infinie, à moins que $\frac{\phi(z)}{z^n}$ ne soit nul quand $z = 0$, pour toute valeur finie de n.

Car si $\frac{\phi(z)}{z^n}$ n'est pas nul quand $z = 0$ pour toute valeur finie de n, soit m une valeur telle que $\frac{\phi(z)}{z^m}$ ne soit pas nul quand $z = 0$. Si $\frac{\phi(z)}{z^m}$ acquiert alors une valeur finie, la proposition est démontrée. Sinon $\frac{\phi(z)}{z^m}$ étant infini et $\phi(z)$ nul pour $z = 0$, en faisant croître n depuis $n = 0$ jusqu'à $n = m$, les valeurs de $\frac{\phi(z)}{z^m}$ pour $z = 0$ devront être infinies à partir d'une certaine limite. Soit p cette limite. $\frac{\phi(z)}{z^p}$ ne sera pas infini pour $z = 0$ mais $\frac{\phi(z)}{z^{p+\mu}}$ le sera, quelque petite que soit la quantité μ. Donc $\frac{\phi(z)}{z^\mu}$ ne saurait être nul pour $z = 0$. La proposition est donc démontrée.

De cette proposition ainsi "démontrée", Galois conclut qu'une fonction $\phi(s)$, qui ne devient pas infinie pour $z = 0$, peut se mettre sous la forme

$$\phi(z) = A + Bz^n + Cz^m + \ldots + Pz^p + z^k\Psi(z),$$

où les exposants positifs $n, m, \ldots, p, k$ vont en croissant, l'exposant k étant aussi grand qu'on veut et la fonction $\Psi(z)$ n'étant ni nulle ni infinie pour $z = 0$.

De la formule du binôme il déduit ensuite le développement de Taylor.

Quant aux fragments qui suivent, j'ai cru devoir les reproduire tels quels, avec une exactitude minutieuse, en conservant l'orthographe, la ponctuation ou l'absence de ponctuation, sans les quelques corrections qui se présentent naturellement à l'esprit. Cette minutie m'était imposée pour les quelques passages où la pensée de Galois n'était pas claire pour moi ; sur cette pensée, les fragments informes que je publie jetteront peut-être quelque lueur. Je me suis efforcé de donner au lecteur une photographie sans retouche.

J. T.

[Première feuille] ([6]).

Permutations. Nombres de lettres m.

Substitutions. Notation.

Période. Substitutions inverses. Substitutions semblables. Substitutions circulaires. Ordre. Autres substitutions.

Groupes. Groupes semblables. Notation.

Théorème I. Les Permutations communes à deux groupes forment un groupe.

Théorème II. Si un groupe est contenu dans un autre, celui-ci sera la somme d'un certain nombre de groupes semblables au premier, qui en sera dit un *diviseur*.

Théorème III. Si le nombre des permutations d'un groupe est divisible par p (p étant premier), ce groupe contiendra une substitution dont la période sera de p termes.

Réduction des groupes, dépendants ou indépendants. Groupes irréductibles.

Des groupes irréductibles en général.

Théorème. Parmi les permutations d'un groupe, il y en a toujours une où une lettre donnée occupe une place donnée, et, si l'on ne considère dans un groupe irréductible que les permutations où une même lettre occupe une même place et qu'on fasse abstraction de cette lettre, les permutations qu'on obtiendra ainsi formeront un groupe. Soit n le nombre des permutations de ce dernier mn ([7]).

Nouvelle démonstration du théorème relatif aux groupes alternes.

Théorème. Si un groupe contient une substitution complète de l'ordre m et une de l'ordre $m - 1$, il sera irréductible.

Discussion des groupes irréductibles. Groupes, primitif et non primitif. Propriété des racines ([8]).

On peut supposer que le groupe ne contienne que des substitutions paires.

Il y aura toujours un système conjugué complet de m permutations quand $m = 4n$ et $4n + 1$, un système conjugué complet de $\frac{m}{2}$ permutations quand $m = 4n + 2$.

Donc $t = m - 2$ dans le premier cas, $t = (m - 2)/2$ dans le second ([9]).

[Deuxième feuille.]

Application à la théorie des fonctions et des équations algébriques. Fonctions semblables. Combien il peut y avoir de fonctions semblables entre elles. M$^{\text{r}}$ Cauchy. Groupes appartenant aux fonctions. Théorème plus général, quand $m > 4$. Quelles sont les fonctions qui n'ont que m valeurs, ou qui ne contenant que des substitutions paires, n'ont que $2m$ valeurs.

Théorème. Si une fonction de m indéterminées est donnée par une équation de degré inférieur à m dont tous les coefficients soient des fonctions symétriques permanentes ou alternées de ces indéterminées, cette fonction sera elle même symétrique, quand $m > 4$.

Théorème. Si une fonction de m indéterminées est donnée par une équation de degré m dont tous les coefficients, etc. ; cette fonction sera symétrique permanente ou alternée par rapport à toutes les lettres ou du moins par rapport $m - 1$ d'entre elles.

Théorème. Aucune équation algébrique de degré supérieur à 4 ne saurait se résoudre ni s'abaisser.

Du cas où une fonction des racines de l'équation dont le groupe est G est connue.

Théorème. Soit H le groupe d'une fonction ϕ des racines, G est

un diviseur de H, ϕ ne dépendra plus que d'une ([10]) équation du $n^{ième}$ degré.

On peut ramener à ce cas celui où on supposerait plusieurs fonctions connues.

Premier cas. Quand le groupe appartenant à la fonction connue est réductible. Cas où une seule permutation lui appartient.

2$^{\text{e}}$ cas. Quand le groupe appartenant à la fonction est irréductible non primitif.

3$^{\text{e}}$ cas. Quand le groupe appartenant à la fonction est primitif m étant premier ([11]).

4$^{\text{e}}$ cas. Quand le groupe appartenant à la fonction est primitif et que $m = p^2$.

5$^{\text{e}}$ cas. Quand le groupe est primitif $m - 1$ étant premier ou le carré d'un nombre premier ([12]).

Note sur les équations numériques.

Ce qu'on entend par l'ensemble des permutations d'une équation.

Du cas où cet ensemble constitue un groupe.

Il n'y a qu'une circonstance où nous ayons reconnu que cela doit nécessairement avoir lieu. C'est celui où toutes les racines sont des fonctions rationnelles d'une quelconque d'entre elles.

Démonstration.

C'est improprement, etc. Du reste, tout ce que nous avons dit est applicable à ce changement près. 1°. théorème. Si une équation jouit de la propriété énoncée, toute fonction des racines invariable par les $m - 1$ substitutions conjuguées sera connue, et réciproquement. 2° Théorème découlant de la réciproque précédente ([13]). Toute équation dont les racines seront des fonctions rationnelles de la première ; jouira de la même propriété. 3° Corollaire. Si a est une racine imaginaire d'une pareille équation et que fa en soit la conjuguée, fx sera en gén´ral la conjuguée d'une racine quelconque imaginaire, x.

On peut passer aisément de ce cas à celui où une racine étant connue, quelques unes en dépendent par des fonctions rationnelles. Car soient

$$x, \quad \phi_1 x, \quad \phi_2(x), \ldots$$

Ces racines, si l'on prend, etc.

Il est aisé de voir que la même méthode de décomposition s'applique au cas où dans l'ensemble des permutations d'une équation, n mêmes lettres occupent toujours n mêmes places (abstraction faite de l'ordre) quand une seule de ces lettres occupe une de ces places, et il n'est pas nécessaire pour cela que l'ensemble de ces permutations constitue un groupe.

([14])

On appelle groupe un système de permutations tel que etc. Nous représenterons cet ensemble par G.

GS est le groupe engendré lorsqu'on opère sur tout le groupe G la substitution S. Il sera dit semblable ;

Un groupe peut être fort différent d'un autre et avoir les mêmes substitutions. Ce groupe en général ne sera pas GS.

Groupe réductible est un groupe dans les permutations duquel n lettres ne sortent pas de n places fixes. Tel est le groupe

$$\begin{array}{ccc} abcde & abdec & abecd \\ bacde & badec & baecd \end{array}$$

Un groupe irréductible, etc.

Un groupe irréductible est tel qu'une lettre donnée occupe une place donnée. Car, supposons qu'une place ne puisse appartenir qu'à n lettres. Alors toute place occupée par l'une de ces lettres jouira de la même propriété. Donc etc.

Groupe irréductible non-primitif est celui où l'on a n places et n lettres telles que une des lettres ne puisse occuper une de ces places, sans que les n lettres n'occupent les n places.

On voit que les lettres se partageront en classes de n lettres telles que les n places en question ne puissent être occupées à la fois que par l'une de ces places ([15]). d'où

$$TS' = STS' = T - 1ST$$

Sur l'autre face du même fragment, on lit :

Si l'on représente les n lettres par n indices

$$1.2.3 \ldots n$$

toute permutation pourra être représentée

$$\phi 1 \quad \phi 2 \quad \phi 3 \ldots \phi n$$

ϕ étant une fonction convenablement choisie la substitution par laquelle on passe de la première perm. à l'autre sera $(k, \phi k)$, k désignant un indice quelconque.

Au lieu de représenter les lettres par des nombres on pourrait représenter les places par des nombres.

. . . . . .

équations ([16]). Nous nous contenterons donc d'avoir exposé les définitions indispensables pour l'intelligence de la suite et nous allons montrer la liaison qui existe entre les deux théories.

§ 2. Comment la théorie des Équations dépend de celle des Permutations.

6. Considérons une équation à coefficients quelconques et regardons comme rationnelle toute quantité qui s'exprime rationnellement au moyen des coefficients de l'équation, et même au moyen d'un certain nombre d'autres quantités irrationnelles adjointes que l'on peut supposer connues a priori.

Lorsqu'une fonction des racines ne change pas de valeur numérique par une certaine substitution opérée entre les racines, elle est dite invariable par cette substitution. On voit qu'une fonction peut très bien être invariable par telle ou telle substitution entre les racines, sans que sa forme l'indique. Ainsi, si $F(x) = 0$ est l'équation proposée, la fonction $\phi[F(a), F(b), \ldots]$, (ϕ étant une fonction quelconque, $a, b, c \ldots$ les racines) sera une fonction de ces racines invariable par toute substitution entre les racines, sans que sa forme l'indique généralement.

Or c'est une question dont il ne paraît pas qu'on ait encore la solution, de savoir si, étant donnée une fonction de plusieurs quantités numériques, on peut trouver un groupe qui contienne toutes les substitutions par lesquelles cette fonction est invariable, et qui n'en contienne pas d'autres.

Il est certain que cela a lieu pour des quantités littérales, puisqu'une fonction de plusieurs lettres invariables par deux substitutions est invariable par leur produit. Mais rien n'annonce que la même chose ait toujours lieu quand aux lettres on substitue des nombres.

On ne peut donc point traiter toutes les équations comme les équations littérales. Il faut avoir recours à des considérations fondées sur les propriétés particulières de chaque équation numérique. C'est ce que je vais tâcher de faire

Des cas particuliers des équations ([17])

Remarquons que tout ce qu'une équation numérique peut avoir de particulier, doit provenir de certaines relations entre les racines. Ces relations seront rationnelles dans le sens que nous l'avons entendu, c'est à dire qu'elles ne contiendront d'irrationnelles que les coefficients de l'équation et les quantités adjointes. De plus ces relations ne devront pas être invariables par toute substitution opérée sur les racines, sans quoi on n'aurait rien de plus que dans les équations littérales.

Ce qu'il importe donc de connaître, c'est par quelles substitutions peuvent être invariables des relations entre les racines, ou ce qui revient au même, des fonctions des racines dont la valeur numérique est déterminable rationnellement.

A ce sujet, nous allons démontrer un théorème de la dernière importance dans cette matière et dont l'énoncé suit : "*Étant donnée une équation avec un certain nombre de quantités adjointes, il existe toujours un certain groupe de permutations dont les substitutions sont telles* ([18]) que toute fonction des racines invariable par ces substitutions est rationnellement connue, et telle réciproquement qu'une fonction ne peut être rationnellement déterminable, à moins d'être invariable par ces substitutions que nous nommerons substitutions de l'équation." *(Dans le cas des équations littérales, ce groupe n'est autre chose que l'ensemble de toutes les permutations des racines, puisque les fonctions symmétriques sont seules connues).*

Pour plus de simplicité, nous supposerons dans la démonstration de notre théorème, qu'il ait été reconnu pour toutes les équations de degrés inférieurs ; ce qu'on peut toujours admettre puisqu'il est évident pour les équations du second degré.

Admettons donc la chose pour tous les degrés inférieurs à m ; pour la démontrer dans le $m^{ième}$, nous distinguerons quatre cas :

1er Cas. L'équation se décomposant en deux ou en un plus grand nombre de facteurs.

Soit $U = 0$ l'équation, $U = VT, V$ et T étant des fonctions dont les coefficients se déterminent rationnellement au moyen des coefficients de la proposée et des quantités adjointes.

Je vais faire voir que, dans l'hypothèse, on pourra trouver un groupe qui satisfasse à la condition énoncée.

Remarquons ici que dans ces sortes de questions, comme il ne s'agit que, des substitutions par lesquelles des fonctions sont invariables, si un groupe satisfait à la condition, tout groupe qui aurait les mêmes substitutions y satisfera aussi. Il convient donc de partir toujours d'une permutation arbitraire, mais fixe, afin de déterminer les groupes que l'on aura à considérer. De cette manière, on évitera toute ambiguïté.

Cela posé, dans le cas actuel, il est clair que si l'on adjoignait à l'équation $U = 0$, toutes les racines de l'équation $V = 0$, l'équation $U = 0$ se décomposerait en facteurs dont l'un serait $T = 0$, et les autres seraient les facteurs simples de V.

Soit H le groupe que l'on obtient en opérant sur une permutation arbitraire A des racines de l'équation $U = 0$, toutes les substitutions qui sont relatives à l'équation $T = 0$ quand on lui adjoint les racines de $V = 0$.

Soit K le groupe que l'on obtient en opérant sur toutes les substitutions qui sont relatives à $V = 0$ quand on ne lui adjoint que les quantités adjointes primitivement à la proposée.

Combinez en tous sens toutes les substitutions du groupe H avec celles du groupe K. Vous obtiendrez un groupe réductible que je dis jouir de la condition exigée relativement à la question proposée.

En effet toute fonction invariable par les substitutions du groupe K ([19] [20])

Soit donc $\phi(H)$ une certaine fonction invariable par les substitutions du groupe H et non par celles du groupe G. On aura donc

$$\phi(H) = f(r)$$

la fonction y ne contenant dans son expression que les quantités antérieurement connues.

Éliminons algébriquement r entre les équations

$$r^p = A \quad f(r) = z$$

On aura une équation irréductible du $p^{ième}$ degré en z. (Sinon z serait fonction de r^p : ce qui est contre l'hypothèse). Maintenant soit S une des substitutions du groupe G qui ne lui soient pas communes à H. On voit que $\phi(HS)$ sera encore racine de l'équation ci-dessus en z, puisque les coefficients de cette équation sont invariables par la substitution S.

On aura donc

$$\phi(HS) = f(\alpha r)$$

α étant une des racines de l'unité.

Ces deux équations

$$\phi(H) = f(r) \quad \phi(HS) = f(\alpha r)$$

donneront par l'élimination de r une relation entre

$$\phi(H) \quad \phi(HS) \quad \text{et } \alpha$$

indépendante de r, et la même relation aura par conséquent lieu entre

$$1 + \phi(H) \quad \text{et} \quad \phi(HS^2)$$

Donc : comme

$$\phi(HS) = f(\alpha r)$$

on en déduit

$$\phi(HS^2) = f(\alpha^2 r)$$

et ainsi de suite, jusqu'à

$$\phi(HS^p) = f(r) = \phi(H)$$

Ainsi la connaissance de la seule quantité r, donne à la fois toutes les fonctions correspondantes aux groupes

$$H, HS, HS^2, ...$$

la somme de ces groupes est évidemment G, puisque toute

Étant donnée ([21]) une équation avec tant de quantités adjointes que l'on voudra, on peut toujours trouver quelque fonction des racines qui soit numériquement invariable par toutes les substitutions d'un groupe donné et ne le soit pas par d'autres substitutions.

Si le groupe d'une équation se décompose en n groupes semblables H, HS, HS ([22]), et qu'une fonction $\phi(H)$ soit invariable par toutes les substitutions du groupe H par aucune autre substitution du groupe G, cette fonction est racine d'une équation irréductible du $n^{ième}$ degré dont les autres racines sont $\phi(HS)$, ...

Note ([23]).

On appelle équations non-primitives les équations qui, étant, par exemple du degré mn se décomposent en m facteurs du degré n au moyen d'une seule équation du degré m. Ce sont les Equations de M^{r} Gauss. Les équations primitives sont celles qui ne jouissent pas d'une pareille simplification. Je suis, à l'égard des Equations primitives, parvenu aux résultats suivants :

1° Pour qu'une équation primitive de degré m soit résoluble par radicaux, il faut que $m = p^{\nu}, p$ étant un nombre premier

2° Si l'on excepte le cas de $m = 9$ et $m = p^{p}$, l'équation devra être telle que deux quelconques de ses racines étant connues, les autres s'en déduisent rationnellement.

3° Dans le cas de $m = p^{p}$, deux des racines étant connues, les autres doivent s'en déduire du moins par un seul radical du degré p.

4° Enfin dans le cas de $m = 9$, l'équation doit être du genre de celles qui déterminent la trisection des fonctions Elliptiques.

La démonstration de ces propositions est fondée sur la théorie des permutations. ([24])

Addition au mémoire sur la résolution des équations.

Lemme I. Soit un groupe G de $mt.n$ permutations, qui se décompose en n groupes semblables à H. Supposons que le groupe H se décompose en t groupes de m permutations, et semblables à K.

Si, parmi toutes les substitutions du groupe G, celles du groupe H sont les seules qui puissent transformer l'une dans l'autre quelques substitutions du groupe K, on aura $n \equiv 1 \pmod{m}$ ou $tn \equiv t \pmod{m}$.

Lemme II. Si μ est un nombre premier, et p un entier quelconque on aura

$$(x-p)(x-p^2)(x-p^3)\dots(x-p^{\mu-1}) \equiv \frac{x^{\mu}-1}{x-1} \left(\mod \ \frac{p^{\mu}-1}{p-1} \right).$$

Ces deux lemmes permettent de voir dans quel cas un groupe primitif de degré p^{ν} (où p est premier) peut appartenir à une équation résoluble par radicaux.

En effet, appelons G un groupe qui contient toutes les substitutions linéaires possibles par les $\frac{p^{\nu}-1}{p-1}$ lettres. (Voyez le mémoire cité.) Soit, s'il est possible, L un groupe qui divise G et qui se partage lui-même en p groupes semblables à K, K ne comprenant pas deux permutations où une lettre occupe la même place. On peut prouver 1° que s'il y a dans le groupe G et hors du groupe L, quelque substitution S qui transforme l'une dans l'autre quelques substitutions du groupe K, cette substitution sera de r termes, r étant un diviseur de $p-1$.

D'après cela, comme le nombre de permutations du groupe G est $\frac{p^{\nu}-1}{p-1}.(p^{\nu}-p^{\nu-1})(p^{\nu}-p^{\nu-2})\dots(p^{\nu}-p^2)(p^{\nu}-p)$

d'après le lemme I, on devra avoir ([25])

$$(p^{\nu}-p^{\nu-1})(p^{\nu}-p^{\nu-2})\dots(p^{\nu}-p^2)(p^{\nu}-p) \equiv p^k r \left(mod \ \frac{p^{\nu}-1}{p-1} \right)$$

D'où l'on voit que ν doit être un nombre premier ([26]). (Lemme II)

$$pr \equiv \nu \left(mod \ \frac{p^{\nu}-1}{p-1} \right)$$

On en déduit quand $\nu > 2 \quad pr = \mu$, savoir $p = \nu$, puisque p et μ sont premiers.

Ainsi, le théorème que j'avais énoncé dans mon mémoire sera vrai dans tout autre cas que dans celui où p serait élevé à la puissance p.

Toujours devra-t-on avoir $r = 1$, et $L = H$. Ainsi même dans le $p^{p^{ième}}$ degré le groupe de l'équation réduite du degré $\frac{p^p - 1}{p-1}$ = devra être de $\frac{p^p - 1}{p-1} p$ permutations. La règle est donc encore fort simple dans ce cas.

il faut comme on voit 1° que $\nu = 1$; 2° que le groupe de la réduite soit de $\frac{p^p - 1}{p-1} p$ = permutations

([27])

Dans un mémoire sur la théorie des Equations, j'ai fait voir comment on peut résoudre une équation algébrique de degré premier m, dont les racines sont $x_0, x_1, x_2, \ldots, x_{m-1}$, quand on suppose connue la valeur d'une fonction des racines qui ne demeure invariable que par les substitutions de la forme (x_h, x_{ak+b}). Or il arrive, par un hasard que nous n'avions pas prévu, que la Méthode proposée dans ce mémoire s'applique avec succès à la division d'une fonction elliptique de première classe en un nombre premier de parties égales. Nous pourrions, à la rigueur, nous contenter de donner cette division, et le problème de la section des fonctions de première classe pourrait être considéré comme résolu.

Mais, afin de rendre cette solution plus générale, nous nous proposerons de diviser une fonction elliptique de première classe en m parties égales, m étant $= p^n$ et p premier.

Pour cela nous étendons d'abord la méthode exposée dans le mémoire cité, au cas où le degré de l'équation serait une puissance de nombre premier. Nous supposerons toujours que les racines soient $x_0, x_1, x_2, \ldots, x_{m-1}$, et que l'on connaisse la valeur d'une fonction de ces racines qui ne demeure invariable que pour des substitutions de la forme $(k, ak + b)$.

Dans cette expression, k et $ak + b$ signifieront les restes minima de ces quantités par rapport à m. Parmi les substitutions de cette forme, que, pour abréger, nous appelerons substitutions linéaires, il est clair que l'on ne peut admettre que celles où a est premier avec m, sans quoi une même $ak+b$ remplacerait à la fois plusieurs k.

Cela posé, passons à la resolution de la classe d'équations indiquée.

§ 1. *Résolution de l'équation algébrique de degré p^n en y supposant connue la valeur d'une fonction qui n'est invariable que par des substitutions linéaires.*

La congruence $k = ak+b$ n'étant pas soluble pour plus d'une seule valeur, on voit clairement que la fonction qu'on suppose connue n'est invariable par aucune substitution dans laquelle deux lettres garderaient un même rang.

Si donc, mutatis mutandis, on applique à ce cas les raisonnements employés dans le mémoire cité, on vérifiera l'énoncé de la proposition qui suit :

"Étant supposée connue la valeur de la fonction en question, une racine s'exprimera toujours au moyen de deux autres, et l'égalité qu'on obtiendra ainsi sera invariable par les substitutions telles que $(k, ak+b)$."

Soit donc $x_2 = f(x_1, x_0)$ on en déduira en général,

$$x_{2a+b} = f(x_{a+b}, x_b),$$

équation qui, appliquée de toutes manières, donnera l'expression d'une quelconque des racines de deux autres quelconques, si l'on a soin d'y substituer successivement les expressions des racines qui entrent dans cette équation.

Cela posé, prennons une fonction symmétrique Φ des racines $x_0, x_p, x_{2p}, x_{3p}, \ldots, x_{(p^{n-1}-1)p}$; il vient

$$\Phi(x_0, x_p, x_{2p}, \ldots) = \Phi_0$$

$$\Phi(x_1, x_{p+1}, x_{2p+1}, \ldots) = \Phi_1$$

$$\Phi(x_2, x_{p+2}, x_{2p+2}, \ldots) = \Phi_2$$

$$- - - - - - - -$$

$$\Phi(x_{p-1}, x_{2p-1}, \ldots) = \Phi_{p-1}$$

et supposons qu'en général $\Phi_{k+p} = \Phi_{p-1}$ Toute fonction des quantités Φ, qui sera invariable par les substitutions linéaires de ces quantités, sera évidemment une fonction invariable par les substitutions linéaires

de $x_0, x_1, x_2, \ldots, x_{m-1}$. Ainsi l'on connaitra à priori toute fonction des quantités, $\Phi_0, \Phi_1, \ldots, \Phi_{p-1}$, invariable par les substitutions linéaires de ces quantités. On pourra donc 1° former l'équation dont ces quantités sont racines (puisque toute fonction symmétrique est à plus forte raison invariable par les substitutions) ; 2° résoudre cette équation.

Il suit de là, qu'on pourra toujours, au moyen d'une équation de degré p, algébriquement soluble, diviser l'équation proposée en facteurs dont les racines seront respectivement

$$x_0, x_p, x_{2p}, x_{3p}, \ldots$$

$$x_1, x_{p+1}, x_{2p+1}, x_{3p+1}, \ldots$$

$$- - - - - - - - - -$$

Comme dans chaque facteur on aura l'expression d'une racine au moyen de deux autres, par exemple, dans le premier,

$$f(x_p, x_0) = x_{2p}$$

et que cette expression sera invariable par toute substitution linéaire, on voit que chaque facteur pourra se traiter comme l'équation donnée, et que le problème, s'abaissant successivement, sera enfin résolu.

On peut en conséquence regarder comme solubles les équations dans lesquelles on connaîtrait la valeur d'une fonction des racines qui ne serait invariable que par des substitutions linéaires, quand le degré de l'équation est une puissance de nombre premier.

Nous pouvons donc passer à la solution du problème général de la section des transcendantes de première classe, puisque, toute fraction étant la somme de fractions dont les dénominateurs sont des puissances de nombres premiers, il suffit d'apprendre à diviser ces transcendantes en p^n parties égales.

§ 2. *Division des transcendantes de première espèce en $m = p^n$ parties égales.*

Nous déterminerons chaque transcendante par le sinus de son amplitude. On pourrait de la même manière prendre le cosinus ou la tangente, et il n'y aurait rien à changer à ce que nous allons dire.

Nous désignerons par (x, y) le sinus de la transcendante somme des transcendantes dont les sinus sont x et y. Si x est le sinus d'une transcendante, $(x)^k$ désignera celui d'une transcendante k fois plus grande.

Il est clair que $(x, -y)$ sera le sinus de la différence des transcendantes qui ont pour sinus, d'après la notation indiquée pour les sommes.

Cela posé, nous commencerons par une remarque sur la nature des quantités qui satisfont à l'équation $(x)^m = 0$.

Si l'on désigne par p l'une de ses racines, il est clair que $(p)^k$ en sera une autre. L'on aura donc une suite de racines exprimée par $p, (p)^2, (p)^3, \ldots, (p)^{m-1}$. Le nombre des racines étant $> m$, soit q une des racines qui ne sont pas comprises dans cette suite, $(q)^l$ sera une autre racine différente de q et des premières. Car, si l'on avait $(p)^k = (q)^t$ on en déduirait $q = (q)^g, g$ étant un nombre entier.

Prenant donc les deux suites $p, (p)^2, \ldots$ et $q, (q)^2, \ldots$ on trouvera pour la formule générale des racines de l'équation $(x)^m = 0$, cette expression

$$((p)^k, (q)^l)$$

Cela posé, supposons que l'on donne à résoudre l'équation $(x)^m = \sin A$, m étant impair et toujours de la forme p^n. Si x est une des racines, il est clair que toutes les autres seront

$$(x, (p)^k, (q)^l)$$

Posons donc en général

$$(x, (p)^k, (q)^l) = x_{k,l}$$

en faisant $x = x_{00}$ nous en déduirons généralement

$$(x_{2a+b,2c+d} - x_{a+b,c+d}) = (x_{a+b,c+d} - x_{b,d})$$

d'où

$$(x_{2a+b,2c+d} = ((x_{a+b,c+d})^2, x_{b,d})$$

Or il est aisé de tirer de cette égalité une expression rationnelle de $x_{2a+b,2c+d}$ en fonction de $x_{a+b,c+d}$ et de $x_{b,d}$. Car si ϕ est l'arc correspondant à l'un quelconque des sinus qui satisfont à l'équation $(x)^m = \sin A$ pour avoir $\cos\phi$ en fonction de $\sin\phi$, il suffit de chercher le plus grand commun diviseur entre les équations $x^2 + y^2 = 1$ et $f(y) = \cos A, f(y)$ étant le cosinus de la transcendante m fois plus grande que celle dont le cosinus est y. On trouverait de même $\Delta\varphi$ en fonction rationnelle de $\sin\varphi$.

Ou pourra donc, par les formules connues, exprimer

$$x_{2a+b,2c+d} = f(x_{a+b,c+d}, x_{b,d})$$

en fonction rationnelle de $x_{a+b,c+d}$ et de $x_{b,d}$

Ce principe posé, démontrons la proposition suivante :

"Toute fonction rationnelle de $x_{0,0}, x_{1,0}, x_{0,1}, \ldots$ invariable par les substitutions de la forme $(x_{k,l}, x_{ak+b,cl+d})$ immédiatement connue."

En effet, on pourra d'abord rendre cette fonction fonction de $x_{0,0}, x_{1,0}, x_{0,1}$ seuls, par l'élimination des autres racines. Cette fonction ne changerait pas de valeur si à la place de $x_{0,0}, x_{1,0}, x_{0,1}, \ldots$ on mettait $x_{0,0}, x_{1,0}, x_{k,l}$, k n'étant pas nul.

Or, comme toute racine de la forme $x_{0,1}$ s'exprime en fonction rationnelle de $x_{0,0}$, et $x_{0,l}$, il s'ensuit que toute fonction symmétrique des racines dans lesquelles le premier indice n'est pas nul sera connue en fonction rationnelle et entière de $x_{0,0}$ et de $x_{0,l}$. Donc la fonction que nous considérions tout à l'heure ne variant pas quand on met pour $x_{1,0}$ l'une quelconque des racines dont le premier indice n'est pas nul, cette fonction sera une fonction de $x_{0,0}$, et de $x_{0,l}$, seuls. On éliminera encore $x_{0,1}$ de cette fonction qui deviendra fonction de $x_{0,0}$ et enfin une quantité connue.

Le principe est donc démontré.

Cela posé soit F une fonction symmétrique de certaines racines de l'équation proposée. Posons

$$F(x_{0,0}, x_{0,1}, x_{0,2}, \ldots) = y_0$$

$$F(x_{1,0}, x_{1,1}, x_{1,2}, \ldots) = y_1$$

$$F(x_{2,0}, x_{2,1}, x_{2,2}, \ldots) = y_2$$

Prenons une fonction de $y_0, y_1, y_2 \ldots$ invariable par les substitutions linéaires de ces quantités. Il est clair que cette fonction sera une fonction des racines x invariable par toute substitution telle que ([28]) $(x_{k,l,ak+b,ck+d})$. Cette fonction sera donc connue. On pourra donc, par la méthode que j'ai indiquée, trouver les valeurs de $y_0, y_1, y_2 \ldots$ et par conséquent décomposer l'équation proposée en facteurs dont l'un ait pour racines $x_{0,0}, x_{0,1}, x_{0,2}, \ldots$

On trouverait de même un facteur de la même équation dont les racines seraient $x_{0,0}, x_{1,0}, x_{2,0}, \ldots$. On pourra donc en cherchant le plus grand commun diviseur de ces deux facteurs avoir $x_{0,0}$, qui est l'une des solutions cherchées. Il en serait de même des autres racines. ([29])

Note 1. sur l'intégration des équations linéaires.

Soit l'équation linéaire à coefficients variables

$$\frac{d^n y}{dx^n} + P\frac{d^{n-1}y}{dx^{n-1}} + Q\frac{d^{n-2}y}{dx^{n-2}} \ldots + S\frac{dy}{dx} + Ty = V$$

Pour l'intégrer supposons que nous connaissions n solutions

$$y = u_1 \quad , = u, \ldots, = u_n$$

de cette équation privée de second membre. La solution complète

$$y = \alpha_1 u_1 + \alpha_2 u_2 + \alpha_3 u_3 + \ldots + \alpha_n u_n$$

qui convient à l'équation privée de second membre, satisfera encore quand on supposera ce second membre, si au lieu de regarder $\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_n$ comme constantes, on les considère comme déterminées par les équations suivantes en $\frac{dx_1}{dx}, \frac{dx_2}{dx}, \ldots \frac{dx_n}{dx}$

$$(1)\begin{cases} u_1\frac{d\alpha_1}{dx}+u_2\frac{d\alpha_2}{dx}+u_3\frac{d\alpha_3}{dx}+\ldots+u_n\frac{d\alpha_n}{dx}=0 \\ \frac{du_1}{dx}\frac{d\alpha_1}{dx}+\frac{du_2}{dx}\frac{d\alpha_2}{dx}+\frac{du_3}{dx}\frac{d\alpha_3}{dx}+\ldots+\frac{du_n}{dx}\frac{d\alpha_n}{dx}=0 \\ \frac{d^2u_1}{dx^2}\frac{d\alpha_1}{dx}+\frac{d^2u_2}{dx^2}\frac{d\alpha_1}{dx}+\frac{d^2u_3}{dx^2}\frac{d\alpha_3}{dx}+\ldots+\frac{d^2u_n}{dx^2}\frac{d\alpha_n}{dx} \\ \ldots \\ \frac{d^{n-1}u_1}{dx^{n-1}}\frac{d\alpha_1}{dx}+\frac{d^{n-1}u_2}{dx^{n-1}}\frac{d\alpha_1}{dx}+\frac{d^{n-1}u_3}{dx^{n-1}}\frac{d\alpha_3}{dx}+\ldots+\frac{d^2u_n}{dx^{n-1}}\frac{d\alpha_n}{dx}=V \end{cases}$$

Il importe d'abord de reconnaître si le dénominateur commun aux valeurs tirées de ces équations peut ou non être nul.

Pour cela j'observe que ce dénominateur est le même que celui des n équations suivantes résolues par rapport à $PQ\ldots ST$

$$(2)\quad\begin{cases} \frac{d^nu_1}{dx^n}+P\frac{d^{n-1}u_1}{dx^{n-1}}+Q\frac{d^{n-2}u_1}{dx^{n-2}}+\ldots+S\frac{du_1}{dx}+Tu_1=0 \\ \frac{d^nu_2}{dx^n}+P\frac{d^{n-1}u_2}{dx^{n-1}}+Q\frac{d^{n-2}u_2}{dx^{n-2}}+\ldots+S\frac{du_2}{dx}+Tu_2=0 \\ \frac{d^nu_3}{dx^n}+P\frac{d^{n-1}u_3}{dx^{n-1}}+Q\frac{d^{n-2}u_3}{dx^{n-2}}+\ldots+S\frac{du_3}{dx}+Tu_3=0 \\ \ldots \\ \frac{d^nu_n}{dx^n}+P\frac{d^{n-1}u_n}{dx^{n-1}}+Q\frac{d^{n-2}u_n}{dx^{n-2}}+\ldots+S\frac{du_n}{dx}+Tu_n=0 \end{cases}$$

Or ces équations doivent être parfaitement déterminées, puisque la forme d'une équation différentielle dépend uniquement de celle de l'équation intégrale.

Donc le dénominateur en question n'est jamais nul.

Mais on peut de plus le calculer d'avance. Soit D le dénominateur. Il est aisé de voir que l'on aura

$$\frac{dD}{dx}=D_n+D_{n-1}+D_{n-2}+D_{n-3}+\ldots+D_1$$

$D1$ étant ce que devient D quand on y substitue partout $\frac{d^nu}{dx^n}$ à la place de $\frac{d^{n-1}u}{dx^{n-1}}$, $Dn-1$ ce que devient D quand on y met $\frac{d^{n-1}u}{dx^{n-1}}$ au lieu de $\frac{d^{n-2}u}{dx^{n-2}}$ et ainsi de suite enfin $D1$ ce que devient D par la substitution de $\frac{du}{dx}$ la place de u

Et comme toutes les parties sont nulles excepté D_n il reste

$$\frac{dD}{dx}=D_n$$

Mais on a d'ailleurs

$$P=-\frac{D_n}{D}$$

Puisque $-Dn$ est le numérateur de l'expression de P tirée de (2).

Donc $D=e^{-\int Pdx}$ valeur cherchée du dénominateur.

On pourrait de cette dernière formule déduire celle que nous avons trouvée plus haut, en considérant une équation linéaire de l'ordre n, comme remplaçant n équations simultanées seulement du premier ordre. Quant à la détermination des numérateurs des quantités inconnues, et à l'examen du cas où l'on n'aurait qu'une partie des solutions de la question, nous n'entrerons pas dans ces détails auxquels le lecteur suppléera au moyen des principes émis plus haut.

RECHERCHE SUR LES SURFACES DU 2$^{\text{d}}$ DEGRÉ ([30]).

Problème ([31]). Étant données dans un parallélépipède les trois arêtes $m, m', m"$, et les angles $\theta, \theta', \theta''$, que font entre elles respectivement m' et $m"$, m et $m"$, trouver l'expression des angles de la diagonale avec les arêtes.

Soit $m = OM, m' = OM', m" = OM"$. Si l'on cherche l'angle POM que la diagonale OP forme avec OM, on aura dans le triangle OPM

$$\cos POM = \frac{m^2 + OP^2 - \overline{PM}^2}{2m.OP}$$

Mais on a par la géométrie

$$\overline{OP}^2 = m^2 + m'^2 + 2m'm'' \cos\theta + 2mm'' \cos\theta' + 2mm' \cos\theta'$$

$$\overline{PM}^2 = m'^2 + m''^2 + 2m'm'' \cos\theta$$

d'où l'on tire

$$m^2 + \overline{OP}^2 - \overline{PM}^2 = 2m(m + m'' \cos\theta' + m'' \cos\theta'')$$

et enfin

$$\cos POM = \frac{m + m'' \cos\theta' + m' \cos\theta''}{OP}$$

On trouvera de même pour les cosinus des angles $M'OP$ et $M"OP$

$$\frac{m + m'' \cos\theta + m \cos\theta''}{OP} \qquad \text{et} \qquad \frac{m'' + m' \cos\theta + m \cos\theta'}{OP}$$

Le problème est donc résolu.

Problème. Trouver pour des axes quelconques la condition de perpendicularité d'une droite et d'un plan.

Prenons à partir de l'origine et suivant certaine direction $OP = 1$. Appelons $m, m', m"$ les coordonnées du point P. Les équations de toute droite parallèle à OP, seront de la forme

$$\frac{x - a}{m} = \frac{y - b}{m'} = \frac{z - c}{m''}$$

Les quantités $m, m', m"$ étant liées par la relation

$$1 = m^2 + m'^2 + m''^2 + 2m'm'' \cos\theta + 2mm' \cos\theta''$$

Cherchons de même l'équation d'un plan perpendiculaire à OP.

Il est évident que si on appelé x, y, z les coordonnées de ce plan, et que l'on projette orthogonalement sur OP ces coordonnées la somme des projections devra être constante. Or on connaît, par le problème précédent, les cosinus des angles de la droite OP avec les axes. L'équation du plan sera donc.

$$\begin{aligned}(m + m' \cos\theta'' + m'' \cos\theta')x + (m' + m \cos\theta'' + m'' \cos\theta)y \\ + (m'' + m \cos\theta' + m' \cos\theta)z + p = 0\end{aligned}$$

Et il est remarquable que le premier membre de cette équation exprime aussi la distance à ce plan d'un point quelconque dont les coordonnées sont x, y, z. Ce qui est évident puisque ce premier membre n'est autre chose que la somme des projections des coordonnées d'un point sur la droite OP, augmentée de la distance du plan à l'origine.

Cela posé, soit l'équation d'une surface du second degré rapportée à des axes obliques

$$Ax^2 + A'y^2 + A''z^2 + 2Byz + 2B'xz + 2B''xy + 2Cx + 2C'y + 2C''z + D = \phi(x, y, z) = 0$$

Lorsqu'on cherche l'équation du plan qui divise également toutes les cordes parallèles à une droite donnée, on substitue l'équation $\phi(x, y, z) = 0$ à la place de x, y, z,

$$x + \rho m \quad y + \rho m' \quad z + \rho m''$$

et les racines de l'équation en ρ qu'on obtient ainsi, expriment les distances du point (x, y, z) aux deux points où une corde parallèle à la droite $\frac{x}{m} = \frac{y}{m'} = \frac{z}{m''}$ menée par le point (x, y, z) coupe la surface du

second degré. Ces deux distances devant être égales et de signe contraire, il suffira de faire dans l'équation en ρ le second terme nul pour avoir l'équation du plan diamétral.

Or l'équation en ρ est en faisant

$$M = \phi(m, m', m'')$$

$$\begin{aligned} MP = (Am + B''m' + B'm'')x \quad & +(A'm' + b''m + Bm'')y \\ & +(A''m'' + B'm + Bm')z + Cm + C'm' + C''m'' \end{aligned}$$

de la forme

$$\rho^2 + 2P\rho + Q = 0$$

Si l'on cherche l'équation d'un plan principal, il faudra de plus que le plan représenté par $P = 0$ soit perpendiculaire à la droite $\frac{x}{m} = \frac{y}{m'} = \frac{z}{m''}$ et par conséquent que son équation soit de la forme

$$\begin{aligned} (m + m'\cos\theta'' + m''\cos\theta')x + (m' + m\cos\theta'' + m''\cos\theta)y \\ + (m'' + m\cos\theta' + m''\cos\theta)z + p = S = 0 \end{aligned}$$

Il faudra donc que les coefficients de MP et ceux de S soient proportionnels et que l'on ait

$$\frac{MP}{S} = \text{const} = s$$

La quantité étant telle que l'on ait

$$\begin{aligned} (A - s)m + (B'' - s\cos\theta'')m' + (B' - s\cos\theta')m'' = 0 \\ (A' - s)m' + (B'' - s\cos\theta'')m + (B - s\cos\theta)m'' = 0 \\ (A'' - s)m'' + (B' - s\cos\theta')m + (B - s\cos\theta)m'' = 0 \end{aligned}$$

On en déduit l'équation en s,

$$\begin{aligned} 0 =& (A - s)(B - s\cos\theta)^2 + (A' - s)(B' - s\cos\theta')^2 + (A'' - s)(B'' - s\cos\theta'')^2 \\ & - (A - s)(A' - s)(A'' - s) - 2(B - s\cos\theta)(B' - s\cos\theta'') \end{aligned}$$

qui est du troisième degré parce qu'en effet il existe trois plans principaux.

Mais la quantité s et l'équation qui la détermine jouissent d'une propriété fort remarquable que personne jusqu'ici ne paraît avoir observée.

Supposons que l'on transforme les coordonnées en exprimant les anciennes coordonnées d'un point en fonction des nouvelles. Si on substitue les valeurs de x, y, z en x', y', z' dans la fonction $\varphi(x, y, z)$ on obtient une fonction $\varphi'(x', y', z')$ d'une autre forme, et qui est telle que dans la fonction φ on substitue les anciennes coordonnées d'un point déterminé, et dans la fonction φ' les nouvelles, les deux résultats ainsi obtenus sont égaux.

Cela posé reprenons l'expression de s, $s = \frac{MP}{S}$ la quantité M étant le résultat de la substitution des coordonnées du point pris sur une droite fixe à une distance $= 1$ de l'origine c'est à dire d'un point fixe, dans l'équation de la surface, ne variera pas quand on transformera les coordonnées.

La quantité P exprimant la demi-somme des distances d'un point (x, y, z) à la surface distances comptées suivant une droite fixe, est aussi invariable par la transformation des coordonnées. Enfin la quantité S exprimant la distance d'un point à un plan déterminé, ne saurait non plus varier.

La quantité s est donc elle même invariable pour un même plan principal, et l'équation qui donne ses trois valeurs aura des coefficients invariables. Or en la développant, on a

$$\begin{aligned} & (1 - \cos^2\theta - \cos^2\theta' - \cos^2\theta'' + 2\cos\theta\cos\theta\cos\theta'')s^3 \\ & - s^2[A\sin^2\theta + A'\sin^2\theta' + A''\sin^2\theta'' + 2b(\cos\theta'\cos\theta'' - \cos\theta) \\ & + 2B'(\cos\theta\cos\theta'' - \cos\theta') + 2B''(\cos\theta\cos\theta' - cos\theta'')] \\ & + s(A'A'' + AA'' + AA' - 2AB\cos\theta 2A'B'\cos\theta' - 2A''B''\cos\theta'' \\ & - B^2 - B'^2 - B''^2 + 2B'B''\cos\theta \\ & + 2BB''\cos\theta' + 2BB'\cos\theta'') + AB^2 + A'B'^2 + A''B''^2 - AA'A'' - 2BB'B'' = 0 \end{aligned}$$

Divisant tous les coefficients par le premier ou par le dernier on aura trois fonctions des constantes qui entrent dans l'équation de la surface, invariables par la transformation des coordonnées. Si l'on suppose cos $\theta, \cos\ \theta'$ et cos θ" nuls on aura pour tous les systèmes d'axes où cela peut être c'est à dire d'axes rectangulaires,les équations

$$A + A' + A'' = \text{const}$$

$$B^2 + B'^2 + B''^2 - A'A'' - AA''AA' = \text{const}$$

$$AB^2 + A'B'^2 + A''B''^2 - AA'A'' - 2BB'B'' = \text{const}$$

Également si l'on suppose encore dans l'équation en s, B, B', B" nuls, c'est à dire qu'on suppose la surface rapportée à des diamètres conjugués, en divisant toute l'équation par le dernier terme, on trouvera pour tous les systèmes semblables

$$\frac{1 - \cos^2\theta - \cos^2\theta' - \cos^2\theta'' + 2\cos\theta\cos\theta'\cos\theta''}{AA'A''} = \text{const}$$

$$\frac{\sin^2\theta}{A'A''} + \frac{\sin^2\theta'}{AA''} + \frac{\sin^2\theta''}{AA'} = \text{const}$$

$$\frac{1}{A} + \frac{1}{A'} + \frac{1}{A''} = \text{const}$$

Et comme $\frac{1}{A}, \frac{1}{A'}, \frac{1}{A''}$ expriment dans ce cas les carrés des diamètres, on retrouve ici les théorèmes connus.

FIN.

---

1. Trois de ces feuilles comportent du texte ; une se rapporte à la théorie de la transformation, une autre au théorème d'addition pour la fonction sin am, déduit de la formule fondamentale de trigonométrie sphérique, la troisième au théorème d'addition pour la fonction $\Pi(u, a)$.

2. Les papiers que m'a remis Mme de Blignières contiennent un brouillon, couvert de ratures et de corrections, qui est de la main de Liouville, et qui porte en tête : Lettre d'Alfred Galois à M. Jacobi, 17 novembre 1847. Voici cette lettre :
   Monsieur,
   J'ai l'honneur de vous envoyer, en vous priant d'en agréer l'hommage, un exemplaire de la première Partie des Œuvres mathématiques de mon frère. Il y a près d'un an qu'elle a paru dans le Journal de M. Liouville, et, si je ne vous l'ai pas adressée plus tôt, c'est que, sans cesse, j'espérais pouvoir vous faire remettre d'un jour à l'autre l'Ouvrage complet, dont la publication s'est trouvée retardée par diverses circonstances. Au reste, cette première Partie renferme ce que mon pauvre Évariste a laissé de plus important et nous n'avons guère à y ajouter que quelques fragments arrachés au désordre de ses papiers. Ainsi on n'a rien retrouvé concernant la théorie des fonctions elliptiques et abéliennes ; on voit seulement qu'il s'était livré la plume à la main à une étude approfondie de vos Ouvrages. Quant à la théorie des équations, M. Liouville et d'autres géomètres que j'ai consultés affirment que son Mémoire, si durement repoussé par M. Poisson, contient les bases d'une doctrine très féconde et une première application importante de cette doctrine. "Ce travail, me disent-ils, assure pour toujours une place à votre frère dans l'histoire des Mathématiques." Malheureusement étranger à ces matières, j'écoute avec plaisir de telles paroles : si votre précieux suffrage, qu'Évariste aurait ambitionné par-dessus tout, venait les confirmer, ce serait pour ma mère et pour moi une bien grande consolation ; il deviendrait pour notre Évariste un gage d'immortalité, et je croirais que mon frère n'est pas entré tout entier dans la tombe. Etc., etc.

3. En posant
   $$[m, n] = \int_0^1 (1-x)^{m-1} x^{m-1}\, \mathrm{d}x,$$
   Galois part de la relation $[m+1, n] = \dfrac{m}{m+n}[m, n]$;
   il en déduit, en désignant par p un nombre entier positif quelconque,
   $$[m, n] = \frac{[p, m]}{[p, m+n]}[m+p, n],$$
   puis
   $$[m, n] = \lim_{p\to\infty} \frac{[p, m] \times [p, n]}{[p, m+n]};$$

remplaçant $[p,n]$ par $\dfrac{1}{p^n}\displaystyle\int_0^p (1-\int xp)^{\mu-1}x^{n-1}\,\mathrm{d}x$, et en passant à la limite, il obtient $[m,n]=\dfrac{\Gamma m\Gamma n}{\Gamma(m+n)}$.
Il établit ensuite la relation

$$\int_0^1 \frac{x^{n-1}-1}{x-1}\,\mathrm{d}x=\phi(n)-\phi(1),$$

où

$$\phi(n)=\frac{d\log\Gamma(n)}{dn},$$

en partant de ce que l'on a, pour $m=1$,

$$\frac{d\log[m,n]}{dm}=\frac{\int_0^1\log(1-x)x^{n-1}\,\mathrm{d}x}{\int_0^1 x^{n-1}\,\mathrm{d}x}=\int_0^1\log(1-x)nx^{n-1}\,\mathrm{d}x,$$

d'où, en intégrant le dernier membre par parties,

$$\phi(1)-\phi(n+1)=-\int_0^1\frac{x^n-1}{x-1}dx.$$

4. Œuvres d'Abel, édition Sylow, t. I, p. 515.
5. La feuille a été pliée ; sur la moitié de la quatrième page, on trouve quelques calculs relatifs à l'intégrale

$$\int\frac{dx}{\sqrt{x(x^2-2\alpha x+\gamma^2)(x^2-2\beta x+\gamma^2)}}$$

où Galois fait la substitution

$$x+\frac{\gamma^2}{x}=2z$$

6. Ce fragment occupe deux feuilles, écrites sur les deux faces, du format 23 x 18.
7. Cette phrase elliptique a été ajoutée dans une fin de ligne et dans l'interligne au-dessous.
8. La première page finit ici ; les six lignes qui suivent sont au verso.
9. Un peu plus bas, on lit : Discussion des groupes irréductibles ; le texte de la page est couvert de calculs, écrits en renversant la page de haut en bas.
10. Les mots mis ici entre crochets sont barrés ; au reste tout ce passage, à partir de "Du cas ou" jusqu'à "plusieurs fonctions connues" est couvert de ratures et de surcharges ; on lit, par exemple, sous une rature : "Si D est le commun diviseur à ce groupe et à celui de la fonction supposée" ; tout ce passage est un renvoi placé au bas de la page, de façon à être substitué à trois lignes qui sont barrées, et dont voici le texte :
Du cas où une fonction des racines est censée connue. Remarque. On peut réduire à ce cas celui où on supposerait plusieurs connues.
11. Au-dessous en interligne :
Jusqu'ici on avait cru
12. Les deux fragments qui suivent sont sur l'autre face de la feuille ; ils sont séparés par un blanc laissé au milieu de la page ; au-dessus de l'avant-dernière ligne du premier passage et dans le blanc, on trouve les mots suivants dont le premier est couvert d'une rature et dont les autres sont bâtonnés ; la lecture du mot Présenté est douteuse.

Mémoire
la théorie des fonctions et sur celle
des équations littérales.
Présenté à l'Institut par
E. Galois.
Octobre 1829.

13. Mots placés en interligne et presque illisibles ; on pourrait aussi bien lire *remarque* que *réciproque*.
14. Une feuille du format 23 x 17, écrite sur les deux faces.
15. En renversant la page, on trouve quelques lignes relatives à la décomposition d'un groupe, que l'absence de contexte rend inintelligibles, puis le commencement d'une question, qu'on retrouve en entier sur un petit fragment de papier, comme il suit :
Étant donnée une substitution S et deux permutations A et A' on demande une substitution S' telle que la lettre située au k$^{\text{ième}}$ rang dans A' prenne le $\phi k^{\text{ième}}$ rang dans AS, la lettre située au $k^{ième}$ rang dans A' prenne le $\phi k^{\text{ième}}$ dans $A'S'$.
Supposons le problème résolu. Soit $A'=AT$, on aura évidemment

$$A'S'=AST$$

16. Ce fragment comporte trois feuilles du format 20×15, du même papier que le fragment M ; la troisième feuille, dont il est question dans une note ultérieure, est intacte ; les deux autres sont déchirées, à droite, de haut en bas ; il manque quelques lettres et, parfois, des mots entiers ; d'où les crochets que l'on trouvera dans le texte imprimé. La déchirure a pu se faire en détachant les trois feuilles d'un cahier pareil à celui qui porte le titre "Notes de mathématiques" et dont j'ai parlé plus haut.
Cet essai est sans doute antérieur à la rédaction du Mémoire sur les conditions de résolubilité des équations par radicaux, et de la feuille relative à la proposition I de ce Mémoire, dont j'ai parlé précédemment (p. 11) ; les deux rédactions sont interrompues ; pour l'une et l'autre, la fin de la page reste blanche ; l'essai n'a pas été achevé.

17. Ces mots sont mis en marge.

18. La page se termine au mot “telles”, le reste se continue sur deux feuilles distinctes ; l’une de ces deux feuilles est écrite sur le recto et le verso, c’est celle dont le texte est imprimé ci-dessus ; l’autre feuille n’est écrite que sur le recto, jusqu’au milieu de la page : le verso contient quelques calculs relatifs à la résolution algébrique de l’équation du troisième degré. Les deux feuilles contiennent le même texte jusqu’à la fin de l’alinéa “sont seules connues”. A partir de ces mots, on lit dans la seconde feuille :
Mais, avant de développer la démonstration complète de cette proposition, nous ferons voir qu’il suffit de la donner dans le cas où l’équation proposée ne se décompose pas en facteurs dont les coefficients se déduisent rationnellement de ses coefficients et des quantités qui lui sont adjointes, plus brièvement, dans le cas où l’équation n’a pas de diviseurs rationnels. Admettons en effet que la chose ait été démontrée dans ce cas, et supposons qu’une équation se décompose en deux facteurs qui n’aient eux-mêmes aucun diviseur rationnel.

19. Un fragment qui semble un morceau déchiré (hauteur, 9") d’une feuille de papier du même format contient le texte suivant, d’un côté : Soit G un groupe correspondant à l’équation $\psi = 0$ et $A, B, C...$ les permutations du groupe G. Pour obtenir un pareil groupe, il faut opérer sur une permutation A toutes les substitutions de l’équation ψ. Nous supposons que la permutation A contienne toutes les racines de $F(x) = 0$. Prenons une fonction $\Phi(A\Sigma)$ invariable par les substitutions Σ relatives aux racines de ϕ,
et de l’autre côté :
qui correspondent aux substitutions indiquées quand aux racines de l’équation ϕ on substitue leurs expressions en fonction de celles de ψ. Je dis qu’il viendra un groupe de permutations qui relativement à la proposée $F(x) = 0$ satisfera à la condition exigée. En effet, toute fonction des racines invariable par les substitutions de ce groupe pourra d’abord s’exprimer en fonction des seules racines de l’équation ψ. De plus, comme cette fonction transformée sera encore invariable par les substitutions de l’équation ψ on voit que sa valeur numérique

20. Feuille déchirée (18 x 17), écrite sur les deux faces.

21. Cet énoncé est écrit sur un morceau de papier (10 x 18) ; l’écriture, parfois malaisée à déchiffrer en raison des ratures et des surcharges, trahit une certaine nervosité ; au-dessous, Galois a mis son nom, écrit à main posée, avec une certaine complaisance.

22. Il n’est guère utile de dire qu’il faut lire HS' ; ce passage est à demi effacé.

23. Une seule page de format 20 x 15. Ce fragment et le suivant doivent être rapprochés de l’*Analyse d’un Mémoire sur la résolution algébrique des équations*, qui a été publiée dans le *Bulletin de Férussac (Œuvres*, p. 11), et dont les premières lignes sont identiques à celles du fragment M.

24. Une feuille (18 x 15), écrite des deux côtés.

25. Relativement au premier membre de la congruence qui suit, je dois signaler l’énoncé que voici, écrit sur la première page d’une feuille double (22 x 18) : Le produit

$$(p^\nu - p)(p^\nu - p^2)(p^\nu - p^3)\dots(p^\nu - p^{\nu-1})$$

n’admet point de facteur premier $\dfrac{p^\nu - 1}{\partial(p-1)}$, ∂ étant le plus grand commun diviseur entre ν et $p-1$, à moins que $\nu = 2$.
Cet énoncé est placé au milieu de calculs dont quelques-uns concernent la transformation des fonctions elliptiques. Sur les autres pages, d’autres formules se rapportent à l’équation $\dfrac{du}{dx} = \dfrac{d'u}{dt'}$ aux fonctions trigonométriques, à la résolution des équations binômes, à la décomposition des fonctions trigonométriques en produits ou en fractions simples, etc.

26. Dans la ligne qui suit et, un peu plus loin, dans l’égalité $p = \nu$, la lettre ν a été mise en surcharge sur la lettre μ ; ensuite, la correction n’a pas été faite. Au reste, la lecture de ce fragment est, par endroits, assez difficile.

27. Trois feuilles (20 x 15) écrites sur les deux faces.

28. Il faut lire sans doute

$$(x_{k,l,ak+b,cl+d}).$$

29. Deux pages et demie d’une feuille double (23 x 18).

30. Malgré son caractère élémentaire, j’ai cru devoir publier cette note, qui n’est pas sans intérêt pour l’histoire de la Géométrie analytique et de la théorie des invariants. En raison de son contenu, on peut supposer qu’elle remonte au temps où Galois était élève de M. Richard, dans la classe de Mathématiques spéciales, ou au moment où il sortait de cette classe pour entrer à l’École Normale. Toutefois, la première supposition semble devoir être écartée : s’il en avait eu connaissance, M. Richard aurait sans doute fait pénétrer dans son enseignement les idées de son élève, qui se seraient diffusées immédiatement. Quoi qu’il en soit, cette note a, comme le morceau précédent, l’aspect d’une copie d’écolier, avec la signature en haut et à gauche ; elle ressemble tout à fait à quelques-unes des copies de Galois, que M. Richard avait conservées et données à Hermite. M. Émile Picard a retrouvé ces copies de Galois dans les papiers d’Hermite ; il a bien voulu me les remettre pour qu’elles soient jointes au précieux trésor que Mme de Blignières donne à l’Académie des Sciences. L’une de ces copies contient un petit travail, que Galois a sans doute fait librement et remis à son maître, et où son esprit philosophique se manifeste déjà ; j’en extrais cette curieuse réflexion :
Un auteur me dit : “l’arithmétique est la base de toutes les parties des Mathématiques, puisque c’est toujours aux nombres qu’il faut ramener les résultats des calculs.” D’après la dernière phrase de l’auteur, il serait plus naturel de croire que l’arithmétique est le terme et le complément de l’Analyse ; et c’est ce qui a lieu.
Toutes ces copies, comme la présente note, sont sur du papier de format 23 x 18.

31. Il y a une figure en marge, dans le texte de Galois.