Dossier 27 : feuillets 252 – 285

251 bis

27

Manuscrits de Joseph Liouville
trouvé avec les papiers de Galois
Lettre d'Alfred Galois à Jacobi.

Lettre d'Alfred Galois à M. Jacobi, 17 9^{bre} 1847. 252

Monsieur

J'ai l'honneur ~~de~~ de vous envoyer, en vous priant d'en agréer l'hommage, un exemplaire de la première partie des Œuvres mathématiques de mon frère. ~~L'ouvrage complet vous sera~~ [illegible] ~~L'ouvrage complet, dont la publication a été retardée par diverses circonstances, vous sera remis plus tard.~~ [illegible] ~~La première partie~~ [illegible] ~~Mais je~~ [illegible] ~~que j'espérais d'abord pouvoir vous faire remettre,~~ [illegible] ~~dont la~~

Il y a près d'un an qu'elles ont paru ~~[illegible]~~ dans le Journal de Mathématiques, et si je ne vous l'ai pas adressé plus tôt, c'est que j'espérais ~~pouvoir~~ [illegible] vous faire remettre ~~[illegible]~~ l'ouvrage complet, dont la publication ~~[illegible]~~ s'est trouvée retardée par ~~[illegible]~~ diverses circonstances. Au reste cette première partie renferme ce que mon pauvre ~~frère~~ Evariste a laissé de plus important, et nous n'avons guère à y ajouter que quelques fragments ~~[illegible]~~ arrachés au désordre de ses papiers. ~~[illegible]~~ Ainsi on n'a rien ~~[illegible]~~ retrouvé ~~[illegible]~~ concernant la théorie des fonctions elliptiques et abéliennes, ou ~~l'on voit seulement~~ qu'il s'était livré ~~[illegible]~~ la plume à la main une

Sans cesse

jour à l'autre

s'est trouvée

à une ~~étude~~ approfondie de vos ouvrages. [illegible]

~~d'autres géomètres~~

Quant à la théorie des équations, M. Liouville et d'autres géomètres que j'ai consultés ([illegible]) m'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. [illegible] usage, [illegible]

Malheureusement étranger à ces matières, j'écoute avec plaisir ce langage, [illegible] de telles paroles : si votre frère, [illegible] suffrages venaient les confirmer [illegible] à l'avance [illegible] j'ai appris [illegible] (la tombe)

~~d'attendre d'espérer~~ [illegible], ce serait pour ma mère et pour moi une bien grande consolation ; il deviendrait pour notre Évariste un gage d'immortalité, et je croirais enfin [illegible], que mon frère n'est pas entré tout entier dans la tombe. &c.

(ce qu'Évariste aurait ambitionné par dessus tout)

Brouillon de Liouville pour l'avertissement qu'il a mis en tête des oeuvres mathématiques d'Évariste Galois

Journal de M. p. et a.

t. XI. 1846 - p. 381

Œuvres mathématiques d'Évariste Galois.

Avertissement.

Le Géomètre ingénieux et profond dont nous donnons ici les œuvres, est mort ayant vingt ans à peine; et encore a-t-il dépensé stérilement dans les agitations de la politique, au milieu des clubs ou sous les verrous de Sainte Pélagie, la plus grande partie des deux dernières années d'une vie si courte. Il était né le ...., et au mois de Mai 1832 un fatal duel l'enleva aux Sciences mathématiques dont il aurait de jour en jour reculé les limites. Le principal travail de Galois est relatif à la résolubilité des équations par radicaux. L'auteur y pose les bases d'une théorie générale qu'il applique en détail aux équations irréductibles de degré premier. Dès l'âge de seize ans et sur les bancs du Collège Louis le Grand, où ses dispositions furent encouragées par un excellent Professeur, par un excellent homme, M. Richard (*), Galois s'était occupé de ce sujet difficile. Il présenta successivement à l'académie plusieurs mémoires contenant les résultats de ses méditations; mais, à part quelques fragments, il ne nous reste aujourd'hui que l'écrit composé en dernier lieu sous la date du 16 janvier 1830. Les Commissaires chargés du rapport reprochèrent au jeune analyste une rédaction obscure, et ce reproche, [redacted] qu'on avait adressé déjà (Galois lui-même nous l'apprend) à ses précédentes communications, était fondé, nous devons l'avouer. Un désir exagéré de concision fit [redacted] souvent tomber Évariste

(*) M. Le Verrier, M. Hermite, et d'autres savants distingués ont suivi aussi la classe de M. Richard. Les bons élèves font la gloire du maître.

$V,\ \varphi V,\ \varphi^2 V,\ \dots\ \varphi^{n-1} V.$

$$\begin{cases} x_0 = \lambda(V) \\ x_1 = \lambda(\varphi V) \\ x_2 = \lambda(\varphi^2 V) \\ x_3 = \lambda(\varphi^3 V) \\ \vdots \\ x_{n-1} = \lambda(\varphi^{n-1} V). \end{cases}$$

μn

$(\mu-1)n+1$

$= \mu n - (n-1).$

$x^5 - x + 1 = p$

$x^p = 1$

$x^n = 1$

$x^2 = -1.$

$V,\ \varphi V,\ \varphi^2 V,\ \dots\ \varphi^{n-1} V,$

$V_1,\ \varphi V_1\ \ \varphi^2 V_1,\ \dots\ \varphi^{n-1} V$

$V_2,\ \varphi V_2,\ \dots\ \varphi^{n-1} V_2$

$V_1 = \varpi V.$

$x_0\ \ x_1\ \ x_2 \dots\dots x_{n-1},$

$x_0\ \ x_1\ \ x_c \dots\dots x_l.$

$x_a\ \ x_b$

[redacted]

$x_0\ x_1\ x_2\ x_3\ x_4$

$\parallel\ x_a\ x_b\ x_c\ x_d\ x_e.$

$x_f\ x_c\ x_d\ x_e\ x_a$

$x_0\ x_1\ x_2 \dots x_{n-1}$

$x_{f(0)}\ x_{f(1)}\ x_{f(2)} \dots x_{f(n-1)}$

[redacted]

Une notice nécrologique sur Galois (par M. Auguste Chevalier) a paru dans le même numéro. Elle contient des détails intéressants. Certains jugements trop absolus, certaines assertions un peu exagérées devront sans doute rencontrer des contradicteurs. Mais l'auteur a d'avance trouvé son excuse et dans sa grande jeunesse et dans la tendre amitié qui l'unissait à Galois.

Mr. Galois,
rue d'enfer, 61.

Mr. William Thomson, St Peters college, (Cambridge)
(n°. 31, rue Monsieur le Prince, chez Mr. Bitty)

Fin du Cours d'Analyse indiquée au 10 avril 1845,
Examens généraux du 21 au 25.

Mr. Debain (mardi, jeudi, samedi) — 1ère leçon au jeudi 10 avril.

... du Luxembourg, N°. 22

Puissent les Géomètres trouver que j'ai accompli la promesse que je faisais à l'Académie des Sciences dans sa séance du 4 juillet 1843 en m'exprimant ainsi (Comp. rend. t. 17, p. 448):

« A la suite d'une discussion où l'on a tant parlé d'équations algébriques, j'espère intéresser l'Académie en lui annonçant que dans les papiers de d'Evariste Galois (qui m'ont été confiés par M. Auguste Chevalier), j'ai trouvé ~~la~~ une solution aussi exacte que profonde de ce beau problème : Etant donnée une équation irréductible de degré premier, décider si elle est ou non résoluble par radicaux. Le Mémoire de Galois est rédigé peut-être d'une manière un peu trop concise. Je me propose de le compléter par un commentaire qui ne laissera, je crois, aucun doute sur la réalité de la belle découverte de notre ingénieux et infortuné compatriote. »

4) 258.

<u>Bulletin des Sciences</u> de M. Férussac. Puis viendront les pièces inédites et enfin un commentaire où nous nous proposons de compléter certains détails et d'éclairer quelques points délicats.

La veille de sa mort et dans la prévision du sort funeste qui l'attendait, Galois traça rapidement le résumé des grandes idées dont il était occupé, et ad[illegible]s forme lettre à son meilleur ami, M. Auguste Chevalier, ce dernier écrit, sorte de testament scientifique qu'on ne lira pas sans émotion en songeant dans quelle circonstance il fut composé.

Cette lettre qui servira de Préface aux œuvres posthumes a été inserée dans notre Journal

11,75
11,75
24,95
48,45
1,75
50,20

Œuvres mathématiques d'Evariste Galois.

Avertissement.

Le Géomètre ingénieux et profond dont nous donnons ici les œuvres est mort ayant vingt ans à peine; et encore a-t-il dépensé stérilement dans les agitations de la politique, au milieu des clubs ou sous les verroux de Sainte Pélagie, la plus grande partie des deux dernières années d'une vie si courte. Il était né le ...., et ~~au~~ mois de mai 1832 un fatal duel l'enleva aux sciences mathématiques dont il aurait de jour en jour reculé les limites!

$$\int_0^{\frac{\pi}{2}} \frac{\cos^n\varphi \cos n\varphi \, d\varphi}{a^2\cos^2\varphi + x^2\sin^2\varphi} = \frac{\pi x^{n-1}}{2a(x+a)^n}$$

$$\frac{d^2x}{dt^2} = \frac{dV}{dx}$$

Sur E. Galois

J. Liouville

de E. Galois

J. Liouville

J. Liouville

Notes sur Galois.

Adjonction. — Expression des racines $x_0, \ldots, x_{n-1}$ par V. — V, V' &c s'expriment rationnellement l'une de l'autre. — C'est donc toujours en facteurs de degrés égaux que l'éq. en V se décompose par adjonction.

— Admettons qu'en adjoignant $\underline{r}$ racine d'une éq. irréductible de degré $\underline{p}$, l'éq. en V se décompose $V^m + \&c = f(V,r) f_1(V,r) \cdots f_{q-1}(V,r)$; $f, f_1, \ldots f_{q-1}$ de même degré $\underline{s}$, $sq = m$. — Et aussi $V^m + \&c = f(V,r') f_1(V,r') \ldots$

$f_{q-1}(V,r') = f(V,r'') f_1(V,r'') \ldots$, si r', r'' &c sont les autres racines de $r^p + \&c = 0$.

Donc $(V^m + \&c)^p = f(V,r) f(V,r') \cdots f(V,r^{(p-1)})$

$\times f_1(V,r) f_1(V,r') \cdots f_1(V,r^{(p-1)})$

$- - - - - - - - -$

Mais $f(V,r) f(V,r') \ldots f(V,r^{(p-1)})$ est rationnel avant ~~toute~~ adjonction, c'est donc un diviseur rationnel de $(V^m + \&c)^p$, et à cause du degré et de $m = sq$, c'est $(V^m + \&c)^s$. Donc

$(V^m + \&c)^s = f(V,r) f(V,r') \ldots f(V,r^{(p-1)})$.

Mais si $f(V,r)$ et $f(V,r')$ ont un facteur commun, ils coïncident, car soient $\varphi(V), \psi(V)$, &c les racines (outre V) de $f(V,r) = 0$. Alors $f(\varphi V,r) = f(V,r) Q(V,r)$. Donc $f(\varphi V,r') = f(V,r') Q(V,r')$, et si $f(V,r') = 0$, il suit $f(\varphi V,r') = 0$. Donc &c. — Il y a donc $\underline{s}$ facteurs qui coïncident avec $f(V,r)$, &c. — Et $V^m + \&c = f(V,r) f(V,r_1) \ldots f(V,r_{q-1})$

$= f(V,r) f_1(V,r) \cdots f_{q-1}(V,r)$.

De là deux genres bien distincts de décomposition. Mais si toutes les racines $r, r_1, \ldots, r_{q-1}$ s'expriment rationnellement par une seule d'entre elles, il est visible que le 1er genre de décomposition rentre dans le second, et que les deux genres de décomposition coïncident.

Au moment où nous adjoindrons une racine $\sqrt[p]{A}$, nous aurons le droit de supposer déjà adjointes les racines de $\alpha^p = 1$ qui dépendent de radicaux d'ordre inférieur, et dès lors les racines de $r^p = A$ sont toutes exprimables rationnellement par une seule. D'ailleurs si l'éq. $r^p = A$ ne restait pas irréductible, et si $r^q + \&c \ldots - H = 0$ était un de ses facteurs, les racines de ce facteur donneraient par leur produit $\alpha^a r . \alpha^b r \ldots = H$, $r^q = K$, en sorte que $\underline{r}$ serait une racine de degré $\underline{q}$, non de degré $\underline{p}$, comme on le suppose. Ainsi on s'en tenant au degré $\underline{p}$ premier, les théorèmes ci-dessus s'appliqueront à ce mode d'adjonction.

Par une suite d'adjonctions de radicaux de degré 1^er^ l'éq. $f(x)=0$ finit par s'abaisser du degré $\underline{n}$ (que je suppose premier) à un degré moindre. Soit $r=\sqrt[p]{A}$ le radical qui produit cet abaissement, $\underline{p}$ ayant la plus petite valeur possible, en sorte que l'abaissement n'aurait pas lieu en adjoignant α racine de $\alpha^p=1$, et qu'après cette adjonction de α l'éq.^on^ $\xi^p=A$ reste irréductible. — Soit $f(x,r)$ le plus facteur (quant au degré en $\underline{x}$) de $f(x)$; $f(x,r')=f(x,\alpha r)$, $f(x,\alpha^2 r)$, … en seront d'autres et seront premiers entr'eux, sans quoi le commun diviseur de deux fournirait un facteur de degré moindre. Donc $f(x,r)f(x,r')$… fait un diviseur de $f(x)$, et exact rationnel sans l'adjonction de $\underline{r}$, donc si $\underline{i}$ est le $=f(x)$. Donc $f(x)=f(x,r)f(x,r')\ldots f(x,r^{(p-1)})$, degré de $f(x,r)$, $ip=n$, donc, pour $\underline{n}$ premier, $i=1$, $p=n$. Pour $\underline{n}$ composé, $\underline{p}$ divise $\underline{n}$. — Ainsi pour $\underline{n}$ premier, l'éq.^on^ s'abaisse en une seule fois au 1^er^ degré.

Mais alors V s'abaisse aussi au 1^er^ degré. Donc V était auparavant de degré $\underline{n}$. Les adjonctions précédentes avaient déjà réduit à $\underline{n}$ son degré primitif $\underline{m}$. Ces adjonctions peuvent se réduire à celle d'une seule quantité $\underline{t}$ dépendant rationnellement des radicaux adjoints et les exprimant rationnellement à son tour.

Dans la dernière éq. en V (de degré $\underline{n}$ premier) les racines ne peuvent ~~être~~ que V, φV, $\varphi^2 V$, …, $\varphi^{n-1}V$, et $\varphi^n V=V$; φV est rationnelle en V dès le commencement avant toute adjonction : car il en résulterait $x_0=\frac{1}{n}(\lambda(V)+\lambda(\varphi V)+\ldots+\lambda(\varphi^{n-1}V))=$ quantité rationnelle avant d'adjoindre $r=\sqrt[p]{A}$. Donc $\lambda(\varphi V)=x_1$, $\lambda(\varphi^2 V)=x_2$, …, $\lambda(\varphi^{n-1}V)=x_{n-1}$. — On voit que le dernier groupe de l'éq.^on^ ne renferme que les permutations tournantes. on a $x_0=\lambda(V)$, et on ne peut avoir $\lambda(V)=\lambda(\varphi V)$;

Mais : 1°. On passe d'un groupe à l'autre par une même substitution, savoir en changeant V en V', et les substitutions sont les mêmes dans chaque groupe. Cela résulte de la double forme

$$F(V) = F(V,t)\,F(V,t_1)\,F(V,t_2) \ldots\ldots$$
$$= F(V,t)\,F_1(V,t)\,F_2(V,t) \ldots\ldots$$

Soit donc $x_k, x_{f(k)}$ la permutation par laquelle on passe du 1er groupe au second. Le second groupe sera

$$x_{f(0)},\ x_{f(1)},\ x_{f(2)},\ \ldots,\ x_{f(k)},\ \ldots$$
$$x_{f(1)},\ x_{f(2)},\ x_{f(3)},\ \ldots,\ x_{f(k+1)},\ \ldots$$
$$\vdots$$
$$x_{f(i)},\ x_{f(i+1)},\ x_{f(i+2)},\ \ldots,\ x_{f(i+k)},\ \ldots$$

— — — — — — — — —

Mais les substitutions doivent être celles du 1er groupe

$$x_0,\ x_1,\ x_2,\ \ldots,\ x_{n-1}$$
$$x_1,\ x_2,\ x_3,\ \ldots,\ x_0$$

— — — — — —

Donc le second groupe déduit par le second moyen doit être

$$x_{f(0)},\ x_{f(1)},\ x_{f(2)},\ \ldots,\ x_{f(k)},\ \ldots$$
$$x_{f(0)+1},\ x_{f(1)+1},\ x_{f(2)+1},\ \ldots,\ x_{f(k)+1},\ \ldots$$
$$\vdots$$
$$x_{f(0)+l},\ \ldots\ldots,\ x_{f(k)+l},\ \ldots$$

— — — — — — — — —

Donc $f(i+k)$ revient à $f(k)+l$, l dépend de i, non de k.
$f(i) = f(0)+l$, $f(2i) = f(i)+l = 2f(0)+l$, $f(3i) = 3f(0)+l$, $\ldots$
$f(\mu i) = \mu f(0)+l$, $f(k) = k\frac{f(0)}{i}+l$, $f(k) = ak+b$. Ainsi il n'y a que des permutations linéaires.

Autrement. $x_0 = \lambda(V)$, $x_1 = \lambda(\varphi V)$, $x_2 = \lambda(\varphi^2 V)$, ..., d'où les permutations tournantes. Que fait la substitution d'une autre racine ϖV du second facteur

$$F(V, t_1) = F_1(V, t) \text{ de } F(V) = F(V,t) F(V, t_1) \dots$$
$$= F(V,t) F_1(V,t) \dots \text{ ?}$$

$F(\varphi V, t) = F(V,t) Q(V,t)$ donne $F(\varphi V, t_1) = F(V, t_1) Q(V, t_1)$.
Donc $\varpi V, \varphi\varpi V, \dots, \varphi^{n-1}\varpi V$ sont les racines de $F(V, t_1) = 0$.
Mais $F_I(\varpi V, t) = F(V,t) P(V,t)$; donc changeant V en φV, &c. ces racines sont encore $\varpi V, \varpi\varphi V, \varpi\varphi^2 V, \dots, \varpi\varphi^{n-1} V$, qui doivent revenir aux précédentes.

Ainsi

$$\varphi\varpi V = \varpi\varphi^b V,$$
$$\varphi^2\varpi V = \varphi\varpi\varphi^b V = \varpi\varphi^{2b} V,$$
$$\varphi^3\varpi V = \varphi\varpi\varphi^{2b} V = \varpi\varphi^{3b} V, \text{ \&c.}$$

Soit $x_0 = \lambda(V)$, $x_1 = \lambda(\varphi V)$, &c. Changeant V en ϖV,

x_0 se change en $\lambda(\varpi V) = x_a = \lambda(\varphi^a V)$

x_1 - - - - - $\lambda(\varphi\varpi V) = \lambda(\varpi\varphi^b V) = \lambda(\varphi^{a+b} V) = x_{a+b}$,

x_2 - - - — $\lambda(\varphi^2\varpi V) = \lambda(\varpi\varphi^{2b} V) = \lambda(\varphi^{a+2b} V) = x_{a+2b}$,

⋮

x_{n-1} - —— — - —— $x_{a+(n-1)b}$.

En général x_k en x_{a+bk}, ou, si l'on veut, x_{ak+b} comme ci-dessus.
— On voit qu'il y a deux marches bien distinctes à suivre.

1°. Si tout ce qui précède a lieu, en se donnant deux des racines, on se donne visiblement toutes les autres. En effet si on remarque que $x_0 = \lambda(V)$ soit une éq. satisfaite, on ne peut prendre que x_k, x_{ak}, et alors pour k différent de zéro, x_k change de place. Donc si on se donne en outre $x_1 = \lambda(\varphi V)$, il n'y aura qu'une seule racine V qui reste possible, et $x_1, x_2, \dots$ s'expriment par x_0 et x_1 rationnellement. — Mais la réciproque? si les racines dépendent de deux x_0, x_1, l'éq. en V est au plus de degré $n(n-1)$. Soit m son degré. Soit $x = \lambda(V)$ une des racines de $f(x) = 0$. L'éq. $\Pi[x - \lambda V] = (x - \lambda(V))(x - \lambda(V')) \dots = 0$ n'a que des racines appartenant à $f(x)$. Donc $\Pi(x - \lambda V) = f(x)^{\mu}$ et $m = n\mu$. Mais on voit que m est divisible par n. — Il μ est $\overline{\leqq} n-1$. y aura μ facteurs $x - \lambda V$ pour lesquels $x_0 = \lambda V$, μ pour x_1, $x_2, \dots$ Et de même si on avait pris $\lambda_1 V$ qui exprime x_1 au lieu de $\lambda(V)$ &c. Et les racines qui donnent $x_0 = \lambda(V) = \lambda(V_1) = \dots$ sont (à la 1ère près) différentes de celles qui donnent $x_1 = \lambda_1(V) = \lambda_1(V') = \dots$, car si $V' = V_1$, le changement de V en V_1' ou $V' = V_1$ laisserait deux racines à la même place, toutes par conséquent, ~~on aurait~~ $V = \text{fonct}(x_0, x_1) = V_1$, ce qui est absurde.

Ainsi $\mu - 1$ racines pour lesquelles x_0 ne change pas, puis $(\mu - 1)$ pour lesquelles x_1 ne change pas, &c. en mettant ces racines à la place de V. De là $n(\mu - 1) + 1$ permutations où une des racines garde sa place. Mais cela n'épuise pas les $n\mu$ racines V ou les $n\mu$ permutations du groupe. Il y a donc des permutations pour lesquelles toutes les racines changent de place.

Soit φV une de ces racines, $x_0 = \lambda(V)$ devient $\lambda(\varphi V)$ que j'appelle x_1, puis $\lambda(\varphi^2 V) = x_2, \dots$ jusqu'à $\lambda(\varphi^{s-1} V) = x_{s-1}$, $\lambda(\varphi^s V) = x_0$. Mais alors $\varphi^s V = V$, sans quoi le changement de V en $\varphi^s V$ laissant 2 racines x_1, x_2 à la même place y laisserait toutes les autres, et de là $\varphi^s V = f(\dots, x_0, x_1) = V$, puisque le changement de V en $\varphi^s V$ dans $V = f.R.(x_0, x_1)$ ne change pas le second membre. D'ailleurs si $\lambda(V), \lambda(\varphi V), \dots \lambda(\varphi^{s-1} V)$

265 (6

n'épuisaient pas les n racines x, ces n racines se partageraient en groupes d'un nombre égal de racines, ce qui est impossible, n étant premier. Ainsi $S = n$ et $x_0 = \lambda(V)$, $x_1 = \lambda(\varphi V)$, ... $x_{n-1} = \lambda(\varphi^{n-1}(V))$.

Maintenant soit x_k, $x_{f(k)}$ une des permutations du groupe. On peut y appliquer la permutation tournante qui vient d'être trouvée, et aussi appliquer la permutation ci-dessus sur ces permutations tournantes. De là x_k, $x_{f(k+i)+i'}$, où i et i' ont les n valeurs $0, 1, 2, \ldots n$, De là n^2 permutations qui doivent se réduire à $n\mu$ distinctes, $\mu \leqq n-1$. Donc deux au moins sont égales et $f(k+i) + i' = f(k+i_0) + i'_0$ quel que soit k. $f(k+I) = f(k) + C$, C indépendante de K et $I = i - i_0$ différent de zéro, sans quoi $i' = i'_0$ aussi, et absurdité. De là $f(I) = f(0) + C$, $f(2I) = 2f(0) + C$, . . . , $f(k) = ak + b$. Ainsi nous voilà ramenés aux permutations linéaires, et l'éq. ^{on} se résout.

Notes sur Galois.

Mém. de Petersb. 1811.

Regula facilis problemata diophantea per numeros integros expeditè resolvendi.

Integratio generalis æquationum differentialium linearium cujuscunque gradus et quotcunque variabiles involventium.

„Jam haud difficulter intelligitur, istam formam $\int e^{\beta s}$ omnes plane functiones ipsius s exhibere posse. Quod quo clarius appareat ponamus $s = \log p$, fietque $e^{\beta s} = p^\beta$ et $\int e^{\beta s} = \int p^\beta$. notum autem est omnes functiones ipsius p resolvi posse in series, quarum termini procedant secundum potestates ipsius p.“ (Paraceae?) ... pour les fonct. de 2 variables. —

observationes circa fractiones continuas

$$s = \cfrac{n}{1 + \cfrac{n+1}{2 + \cfrac{n+2}{3 + \cfrac{n+3}{4 + \&c.}}}} = \cfrac{n-1}{1 + \cfrac{n-2}{2 + \cfrac{n-3}{3 + \ldots}}}$$

excepté pour $n=1$.

n entier. la série s'arrête.

1809, 1810. Solutio quæstionis curiosæ ex doctrinâ combinationum. Datâ serie quotcunque litterarum $a, b, c, d, e,$ &c quarum numerus sit n, invenire quot modis earum ordo immutari possit, ut nulla in eo loco reperiatur, quem initio occupaverat.

$$\Pi(n) = (n-1)\big(\Pi(n-1) + \Pi(n-2)\big) \text{ ou mieux}$$

$$\Pi(n) = n\,\Pi(n-1) \pm 1; \quad \begin{matrix} + \text{ pour } n \text{ pair} \\ - \text{ pour } n \text{ impair.} \end{matrix}$$

Primo scilicet considerabimus casum, quo littera b in primo loco locatur: mult. ens. par $(n-1)$: puis a peut être au N°. 2, $\Pi(n-2)$; puis à une autre place. d'où $\Pi(n-1)$ parceque a tient lieu de b.

$$\Pi(n) = 1.2\ldots n\left(\frac{1}{1.2} - \frac{1}{1.2.3} + \cdots \pm \frac{1}{1.2\ldots(n-1)}\right)$$

267.

Soit une fonction $P(x)$ infinie pour $x=\alpha$, $x=\beta$. — $\varphi(x)$ une autre de même espèce et générale nulle pour $\alpha, \beta, \gamma, \delta \ldots$, le plus possible, mais infinie deux fois seulement pour a, b.

$$\varphi(x)\,P(x) \text{ n'est aussi infinie que pour } a, b \text{ et dès lors } = \underline{A\varphi(x)+B}.$$

Soit $\varphi(x)P(x) = C$ et D pour $x = \alpha$ et β. — Cela détermine A et B. Mais $\gamma, \delta \ldots$ donnent $B=0$; reste

$$\varphi(x)P(x) = A\,\varphi(x), \quad P(x)=A.$$

Donc il est absurde d'admettre γ et δ. — Et nos fonctions à deux infinis le sont aussi à deux zéros.

Autre rédaction. Soit $\varphi(x)$ une fonction à deux infinis a, b; elle est à deux zéros au moins, nous le savons; je dis en outre qu'elle l'est à deux au plus. — Car si elle l'est à plus de deux, $\alpha, \beta, \gamma, \ldots$; ~~soit~~ $P(x)$ aux infinis (α, β); le produit

$$\varphi(x)\,P(x)$$

ne l'est qu'aux a et b. donc elle est $= A\varphi(x)+B$. Mais si $\varphi(\gamma)=0$, $B=0$. donc $P(x)=A$, ce qui est absurde. — Ainsi il y deux zéros (α, β) ni plus ni moins; et

$$\varphi(x)P(x) = A\varphi(x)+B.$$

Mais $P(x)$ a aussi deux zéros g, h. Soit

1)

Soit $F(x)=0$ une Eq. de degré premier $\underline{n}$. Elle ne peut devenir réductible que par l'adjonction d'un radical de degré $\underline{n}$ et alors l'Eq. en V doit par cette adjonction se réduire au 1er degré. Elle était donc auparavant de degré n. Soient $V, \varphi V, \ldots \varphi^{n-1} V$ ses racines alors. — Dans son état primitif soit ϖV une des racines de l'Eq. en V. Les radicaux dont l'adj. a pu l'abaisser au degré $\underline{n}$ peuvent être adjoints en une seule fois par la racine $\underline{r}$ d'une eq. qui les exprime rationnellement, et de telle manière que les racines $r, r', \ldots$ soient fonctions rationnelles les unes des autres. De là les deux décomp. $f(V,r)\, f(V,r_1')\ldots$ ou $f(V,r) f_1(V,r)$ &c. qui doivent coïncider, $f(V,r_1')=f_1(V,r)$, &c. Soit ϖV racine de $f_1=0$. $V, \varphi V, \ldots$ racines de $f(V,r)=0$ qui est de degré $\underline{n}$. ϖV est racine aussi de $f(V,r_1)=f_1(V,r)$; [redacted] $f_1(\varpi V,r)=f(V,r)\,q(V,r)$; donc en changeant V en φV, on a $\varpi V, \varpi\varphi V, \ldots \varpi\varphi^{n-1} V$ pour racines de $f_1=0$. Mais $f(V,r)=0$ ayant $V, \varphi V$, &c.; $f(\varphi V,r)=f(V,r)\,q(V,r)$; donc en changeant $\underline{r}'$ en $\underline{r}$, et V en ϖV, $\varphi\varpi V$ est aussi racine, et de même $\varphi^2\varpi V$, &c. Les racines $\varpi V, \varpi\varphi V, \ldots \varpi\varphi^{n-1} V$ reviennent donc à $\varpi V, \varphi\varpi V, \ldots \varphi^{n-1}\varpi V$. Ces racines sont diff. $\varpi V=\varpi\varphi^a V$ donnerait $V=\varphi^a V$; $\varpi V=\varphi^a \varpi V$ donnerait donnerait $\varpi^2 V=\varpi^2\varphi^a V$, &c. d'où $V=\varphi^a V$ en remplaçant par V la racine ϖV ou V'. Car toute fonction comme φ et ϖ est rationnelle sans adjonction.

Soient $x_0, x_1, \ldots x_{n-1}$ racines de la proposée.

$x_0=\theta(V)$, $x_1=\theta(\varphi V)$, $\ldots x_{n-1}=\theta(\varphi_{n-1} V)$. Si on avait $\theta(V)=\theta(\varphi V)$ alors $\theta(V)$ ne changeant pas par les subst. de φV, &c racines de $f(V,r)=0$ serait rationnelle (et de là aussi x_0) par la seule adjonction de $\underline{r}$, ce qu'on ne suppose pas, cette adjonction ~~de r laissant encore l'Eq. en x~~ ~~en x~~ irréductible. — Soit ϖV une ~~autre~~ racine avant toute adjonction de l'Eq. $V^\mu + \&c = 0$

$\theta(\varpi V)=x_a=\theta(\varphi_a V)$, $\theta(\varphi\varpi V)=\theta(\varphi_b V)$, [redacted] $\varphi\varpi V=\varpi\varphi^c V$, $\theta(\varphi\varpi V)=\theta(\varpi\varphi^c V)$ $=\theta(\varphi_{a+c} V)$ en changeant V en $\varphi_c V$ dans $\theta(\varpi V)=\theta(\varphi_a V)$; $\theta(\varphi\varpi V)=\theta(\varphi_{a+c} V)$, $b=a+c$; $\varphi^2\varpi V=\varphi\varpi\varphi^c V=\varpi\varphi^{2c} V$, $\theta(\varphi^2\varpi V)=\theta(\varpi\varphi^{2c} V)=\theta(\varphi_{a+2c} V)$ &c. ainsi: V changé en ϖV, change x_0 en x_a, x_1 en x_{a+c}, x_2 en x_{a+2c}, $\ldots\ldots$ x_k en x_{a+kc}; les substitutions ne sont donc que linéaires. Le reste comme dans Galois.

Galois. $F(V) = V^{\mu} + \&c = 0$, ég. en V devenant réductible par l'adj. de r racine d'ég. irréd. de degré p, $(r', r'', \dots r^{(p-1)}$ les autres racines$)$, $F(V) = f(V, r) f_1(V, r) \dots f_{m-1}(V, r)$; les facteurs f supposés non réductibles sont de même degré i puisque les racines V sont fonctions rationnelles les unes des autres, même avant toute adjonction. — $F(V)^p = \overline{f(V, r) f(V, r') \dots f(V, r^{(p-1)})} \times \overline{f_1(V, r) \dots} \times f_2(V, r) \dots$ Donc $f(V, r) f(V, r') \dots f(V, r^{(p-1)})$ quantité rationnelle divise $F(V)^p$ et doit être de forme $F(V)^q$ en conséquence. —

$F(V)^q = f(V, r) f(V, r') \dots f(V, r^{(p-1)})$; $ip = q$ et $im = \mu$, et q diviseur de p, $mq = p$. L'éq.^{on} $mq = p$ où m est > 1, donne $q = 1$ si p est premier.

1°. p premier, alors $q = 1$, $F(V) = f(V, r) f(V, r') \dots f(V, r^{(p-1)})$ et $F(V) = f(V, r) f_1(V, r) \dots f_{m-1}(V, r)$. Donc $m = p$, et $F(V)$ se décompose en p facteurs de deux manières, par $f(V, r) f(V, r') \dots$ et par $f(V, r) f_1(V, r) \dots$

2°. p composé $= mq$, q diff. de l'unité.

$F(V)^q = f(V, r) f(V, r') \dots f(V, r^{(p-1)})$. Les facteurs du second membre doivent se composer de telle sorte que les racines soient q à q égales. Or si deux facteurs $f(V, r)$, $f(V, r')$ ont une racine commune, je dis qu'ils coïncident. Soient $V, \lambda V, \dots$ les racines de $f(V, r) = 0$, et V ~~[illegible]~~ racine aussi de $f(V, r') = 0$. On a $f(\lambda V, r) = f(V, r) Q(V, r)$ identiquement. Donc à cause de l'irréductibilité de l'éq.^{on} en r, $f(\lambda V, r') = f(V, r') Q(V, r')$. Donc λV est aussi racine de $f(V, r') = 0$. Donc &c. Ainsi les facteurs $f(V, r) f(V, r') \dots$ se groupent q à q identiques, et on a $F(V) = f(V, r) f(V, r_1) \dots f(V, r_{m-1})$ en se bornant aux racines $r, r_1, \dots r_{m-1}$ qui donnent des facteurs essentiellement différents. — Ceci donne la clef nette et simple de ce que dit Galois sur les deux modes de décomposition du groupe total. Si les racines $r, r_1, \dots$ sont fonctions rationnelles d'une seule d'entre elles, adjoindre l'une c'est les adjoindre toutes, et il est aisé de voir que les deux genres de décomposition coïncident. alors en effet $f(V, r_1)$ est de forme $f_1(V, r)$ &c.

3/

Les permutations étant de forme x_k, x_{ak+b} et ne laissant ainsi jamais deux racines à la même place puisque la congruence $ak + b \equiv k \pmod{n}$ où n est premier n'a qu'une racine, il s'ensuit que deux racines étant données les autres s'en déduisent rationn. — C'est le 1er théorème. — N. B. Il ne peut pas se faire qu'en changeant V en V' toutes les racines restent à leur place ; car $V = \text{Fonct}(x_0, x_1, \dots x_{n-1})$, on aurait $V' =$ la même fonct. $= V$ ce qui est impossible. — Autre N. L'éq. binome $x^p = A$ reste irréductible si elle n'a pas de racine rationnelle après l'adj. des radicaux inférieurs ; sans cela si r était racine d'éq.^{on} de degré inf. les racines de cette dernière seraient $r, \alpha r, \dots$ et leur produit donnerait pour r une éq. binome de degré moindre qu'on aurait dû prendre au lieu de $v^p = A$. — Nous arrivons à la réciproque : 1°. les racines x_2, &c dépendant rationnellement de x_0, x_1, l'éq.^{on} en V est de degré $n(n-1)$ au plus, soit ns ce degré, $s < p$. — Supposons $x_0 = \theta(V)$, $x - \theta V = 0$, $\Pi(x - \theta V) = 0$ après l'élimination de V ; cette éq. en x ne peut avoir que les racines de la proposée en x, elle est donc une puissance, et toutes doivent y entrer également. — Ainsi $V, \varpi V, \dots$ donnant x_0, $V', \varpi V', \dots$ en nombre égal donneront x_1, &c. Il y aura s racines $V, \varpi V$, &c. — Maintenant soit V' qui donne x_1, égale à φV, V donnant x_0. $x_0 = \theta(V)$, $x_1 = \theta(\varphi V)$. Si on avait $\theta(\varphi^{\nu} V) = x_0$ après d'avoir $x_0 = \theta(V)$, d'où $\nu = n\rho$, V changé en $\varphi^{\nu} V$ changerait x_0 en $\theta(\varphi^{\nu} V) = x_0 = \theta(V)$, d'où aussi x_1 en x_1 &c., c'est à dire ne changerait rien. Ainsi $\varphi^{\nu} V$ serait déjà revenu $= V$. ~~[illegible]~~ — Nous pouvons ce me semble dire qu'en adjoignant une racine x_0 l'éq.^{on} en V doit s'abaisser au degré ~~[illegible]~~ s et ne conserver que les racines $V, \varpi V$, &c. — Et alors on doit pouvoir passer aisément d'un facteur à l'autre. Mais ceci est encore à éclaircir.

3/ 270

Par $\Pi(x - \theta(V)) = 0$ qui ne peut donner qu'une puissance de $(x\ldots)$, nous apprenons que nn' étant le degré de l'Éq.^{on} en V, il y a n' racines pour lesquelles x_0 ou $x_I \ldots$ restent fixes. Mais de là $(n'-1)n + 1 = nn' - (n-1)$ permutations seulement. Il reste à en trouver $(n-1)$ autres. Il y a donc $n-1$ permutations dans lesquelles aucune des racines ne reste à la même place. Soit φV une racine produisant cet effet, $\varphi V, \varphi^2 V, \ldots \varphi^{s-1} V$. Soit $x_0 = f(V)$, $x_1 = f(\varphi V)$; x_0 devient x_1 par le changement et on ensuite $x_2, x_3 \ldots$ puis on revient à x_0. Alors je dis que la série φ est épuisée, car si $f(\varphi^t V) = f(V)$, $t < s$, alors le changement de t en $\varphi^t V$ laisserait x_0 à la même place et x_1 aussi à cause de $f(\varphi^{t+1}(V)) = f(\varphi V) = x_I$. Or il est impossible que deux racines restent à la même place. En effet ~~toutes alors y resteraient~~ puisque deux racines déterminent les autres. Après ce groupe $x_0 x_1 \ldots$ qui revient à x_0 on en formera un autre du même genre et absolument distinct puis un autre jusqu'à l'épuisement des racines. Mais alors le nombre n des racines ne serait pas premier. Donc il n'y a qu'un groupe et $m = n$.

Ainsi

$$\left.\begin{array}{l} V, \varphi V, \varphi^2 V, \ldots \varphi^{n-1} V \\ \varpi V, \varpi\varphi V, \text{---------} \\ \vdots \quad \text{---------} \end{array}\right\} \quad \begin{array}{l} x_0 = f(V) = f(\varpi V) = \ldots \\ x_1 = f(\varphi V) = f(\varpi\varphi V) = \ldots \\ \text{--- --- ---} \end{array}$$

Voilà les racines V. — ~~C'est d'une permutation tournante que résultent nos $(n-1)$ permutations~~ où les racines ne restent pas toutes à la même place.

~~Maintenant~~ soit $x_0\ x_1\ x_2 \ldots x_{n-1}$
changé en $x_a\ x_b\ x_c \ldots x_l$

Soit pour fixer les idées

$x_0\ x_I\ x_2\ x_3\ x_4$ [illegible] et par exemp. $\partial = 0$.
$x_a\ x_b\ x_c\ x_d\ x_e$

alors par perm. ~~tourn.~~

$x_0\ x_d\ x_e\ x_a\ x_b\ x_c$
[illegible]
$x_c\ x_0\ x_d\ x_e\ x_a\ x_b$
$x_{c+1}\ x_I\ x_{d+1}\ x_{e+1}\ x_{a+1}\ x_{b+1}$

4) Soient $V \mid x_0 \; x_1 \; x_2 \; x_3 \; x_4$

Perm. $x_{f(0)} \; x_{f(1)} \; x_{f(2)} \ldots x_{f(k)} \ldots$

[redacted]) $x_i \; x_{i+1} \ldots x_{i+4}$ par perm. tourn.

puis par la fonction $\mid x_{f(i)}, x_{f(i+1)} \ldots f(i+4)$

c'est la permutation tournante de $x_{f(k)}$.

Ainsi on fait les permutations

$$x_k \mid x_{f(k+i)+i'}$$

Il y en aurait $\underline{n}^2$ en variant $\underline{i}$ et $\underline{i'}$ de 0 à $\underline{n}$. Donc une ~~rentre dans les autres~~ et

$$f(k+i)+i' = f(k+i_0)+i'_0$$

ou

$$f(k+i_0+(i-i_0)) = f(k+i_0)+i'_0-i'$$

$$f(K+c) = f(k)+C.$$

Ce qu'il ~~fallait trouver~~.

$$f(c) = f(0)+C$$
$$f(2c) = f(c)+C = f(0)+2C$$
$$f(ic) = f(0)+iC. \qquad (k, ak+b)$$

Mais soit car, alors c'est insignifiant. ~~Mais~~ dans ce cas $i=i_0$ et $i'=i'_0$, ce qu'on ne ~~doit~~ pas supposer.

$$f(k+i) + i' = f(k+i_0) + i_0'$$

ou

$$f(k + i_0 + (i - i_0)) = f(k+i_0) + i_0' - i'$$

$$f(K + c) = f(K) + C.$$

Ce qu'il fallait trouver.

$$f(c) = f(0) + C$$
$$f(2c) = f(c) + C = f(0) + 2C$$
$$f(3c) = f(0) + 3C.$$

Notes sur Galois.

272 + 277

271 bis

Notes sur Galois

<u>Galois.</u> Adjonction. — Expression des racines $x_0, x_1, \dots x_{n-1}$ par V qui en dépend et dont elles dépendent rationnellement. Si l'on considère à la fois deux quantités V, U jouissant de cette propriété, U et V seront fonctions rationnelles l'une de l'autre, et dépendront d'équations irréductibles de même degré. Aussi quand par une adjonction l'équation en V se décompose, c'est toujours en facteurs de degrés égaux.

Admettons qu'en adjoignant r racine d'une équation irréductible de degré p, $r^p + \&c = 0$, l'éq. $V^m + \&c$ auparavant irréductible se décompose ; $V^m + \&c = f(V,r) f_1(V,r) \dots f_{q-1}(V,r)$, $f, f_1, \dots f_{q-1}$ de même degré s, $sq = m$. Et aussi $V^m + \&c = f(V,r') f_1(V,r') \dots f_{q-1}(V,r') = f(V,r'') f(V,r'') \dots$ si r', $r'' \dots$ sont les autres racines de $r^p + \&c = 0$. Donc

$$(V^m + \&c)^p = f(V,r) f(V,r') \dots f(V,r^{(p-1)})$$
$$\times f_1(V,r) f_1(V,r') \dots f_1(V,r^{(p-1)})$$
$$\dots\dots$$
$$\times f_{q-1}(V,r) f_{q-1}(V,r') \dots f_{q-1}(V,r^{(p-1)})$$

Mais $f(V,r) f(V,r') \dots f(V,r^{(p-1)})$ est rationnel avant toute adjonction ; il est donc un diviseur rationnel de $(V^m + \&c)^p$, [redacted] et à cause du [redacted] degré et de $m = sq$, c'est $(V^m + \&c)^s$. Donc

$$(V^m + \&c)^s = f(V,r) f(V,r') \dots f(V,r^{(p-1)})$$

Mais si $f(V,r)$ et $f(V,r')$ ont un facteur commun, ils coïncident, car soient φV, ψV, &c les racines (autres que V) de $f(V,r) = 0$. Alors $f(\varphi V, r) = f(V,r)\, Q(V,r)$. Donc $f(\varphi V, r') = f(V,r')\, Q(V,r')$ et si $f(V,r') = 0$ il suit $f(\varphi V, r') = 0$. Donc &c. Il y a donc q facteurs qui coïncident avec $f(V,r')$ &c.

et $V^m + \&c = f(V,r) f(V,r_1) \dots f(V,r_{q-1})$,
$= f(V,r) f_1(V,r) \dots f_{q-1}(V,r)$.

De là deux genres bien distincts de décompositions.

— Mais si toutes les racines $x, x_1, \dots x_{q-1}$ s'expriment rationnellement par une seule d'entre elles, il est visible que le premier genre de décomposition rentre dans le second et que les deux genres de décompositions coïncident.

[redacted]

Au moment où nous adjoindrons une racine $\sqrt[p]{A}$, nous aurons le droit de supposer déjà adjointes les racines de $\alpha^p=1$ qui dépendent de radicaux d'ordre inférieur, et dès lors les racines de $r^p=A$ sont toutes exprimables rationnellement par une seule. D'ailleurs si l'Éq.on $r^p=A$ ne restait pas irréductible, et si $r^q+\&c.-H=0$ était un de ses facteurs, les racines de ce facteur donneraient par leur produit $\alpha^\mu r.\alpha^\nu r\ldots=H$, $r^q=K$, en sorte que r serait une racine de degré q, non de degré p, comme on le suppose. Ainsi en s'en tenant au degré p premier, les théorèmes ci-dessus s'appliqueront à ce genre d'adjonction.

Par une suite d'adjonctions de radicaux de degré premier, l'Éq.on $F(x)=0$ finit par s'abaisser du degré n (que je suppose premier) à un degré moindre. Soit $r=\sqrt[p]{a}$ le radical qui produit cet abaissement, p ayant la plus petite valeur possible, en sorte que l'abaissement n'aurait pas lieu en adjoignant une racine de $\alpha^p=1$, et que après cette adjonction de α, $x^p=a$ reste irréductible. Soit $f(x,r)$ le plus petit facteur (quant au degré en x) de $F(x)$; on formera d'autres en faisant $f(x,r')=f(x,\alpha r)$, $f(x,\alpha^2 r)\ldots$ premiers entre eux sans quoi le commun diviseur de deux fournirait un facteur de degré moindre. Donc $f(x,r)f(x,r')\ldots$ étant rationnel sans l'adjonction de r, divise $F(x)$ et $F(x)=f(x,r)f(x,r')\ldots f(x,r^{(p-1)})$; donc si i degré de $f(x,r)$, $ip=n$; donc pour n premier, $i=1$, $p=n$. Pour n composé, p divise n. Ainsi pour n premier, l'Éq.on s'abaisse une seule fois au 1er degré.

Mais alors V s'abaisse aussi au 1er degré. Donc V était auparavant de degré n. Les adjonctions précédentes avaient déjà réduit à n son degré primitif m. Les adjonctions peuvent se réduire à celle d'une seule quantité t dépendant rationnellement des radicaux adjoints et les exprimant rationnellement à son tour.

Dans la dernière Éq.on en V (de degré n premier) les racines ne peuvent être que $V, \varphi V, \varphi^2 V, \ldots \varphi^{n-1} V$, et $\varphi^n V=V$. φV est rationnel dès le commencement avant toute adjonction. On a $x_0=\lambda(V)$ et on ne peut avoir $\lambda(V)=\lambda(\varphi V)$ car il en résulterait $x_0=\frac{1}{n}(\lambda(V)+\lambda(\varphi V)+\ldots+\lambda(\varphi^{n-1}V))$ = quantité rationnelle avant d'adjoindre $r=\sqrt[p]{A}$. Donc $\lambda(\varphi V)=x_1$, $\lambda(\varphi^2 V)=x_2$, $\ldots$ $\lambda(\varphi^{n-1}V)=x_{n-1}$.

3) On voit que le dernier groupe de l'Éq. ~~en~~ ne renferme que des permutations ~~sfurs...~~.

Mais : 1° on passe d'un groupe à l'autre par une même substitution, savoir le changement de v en v', et les substitutions sont les mêmes dans chaque groupe. Cela résulte de la double forme

$$F(V) = F(V,t)\,F(V,t_1)\,F(V,t_2)\ldots$$
$$= F(V,t)\,F_1(V,t)\,F_2(V,t)\ldots$$

Soit donc x_k, $x_{f(k)}$ la permutation par laquelle on passe du 1er groupe au second. Le second groupe sera

$$x_{f(0)},\ x_{f(1)},\ x_{f(2)},\ \ldots\ x_{f(k)},\ \ldots$$
$$x_{f(1)},\ x_{f(2)},\ x_{f(3)},\ \ldots\ x_{f(k+1)},\ \ldots$$
$$\vdots$$
$$x_{f(i)},\ x_{f(i+1)},\ x_{f(i+2)},\ \ldots\ x_{f(i+k)},\ \ldots$$

Mais les substitutions doivent être celles du 1er groupe

$$x_0\ x_1\ x_2\ \ldots\ x_{n-1}$$
$$x_1\ x_2\ x_3\ \ldots\ x_0$$

~~...~~ Donc le second groupe défini par ce second moyen, doit être :

$$x_{f(0)},\ x_{f(1)},\ x_{f(2)},\ \ldots\ x_{f(k)},\ \ldots$$
$$x_{f(0)+1},\ x_{f(1)+1},\ x_{f(2)+1},\ \ldots\ x_{f(k)+1},\ \ldots$$
$$\vdots$$
$$x_{f(0)+l},\ \ldots\ \ldots\ ,\ x_{f(k)+l},$$

donc $f(i+k)$ revient à $f(k)+l$, l dépend de i, non de k.
$f(i) = f(0)+l$, $f(2i) = f(i)+l = 2f(0)+l$, $f(3i) = 3f(0)+l$,
$\ldots f(\mu i) = \mu f(0)+l$, $f(k) = k\dfrac{f(0)}{i}+l$, $f(k) = ak+b$.
Ainsi il n'y a que des permutations linéaires.

4)

__Autrement.__ $x_0 = \lambda(V)$, $x_1 = \lambda(\varphi V)$, $x_2 = \lambda(\varphi^2 V)$, ... d'où des permutations tournantes. Que fait la substitution d'une autre racine ϖV du second facteur $F(V, t_1) = F_1(V, t)$ de $A(V) = F(V,t) F(V,t_1) \dots$
$= F(V,t) F_1(V,t) \dots$

$F(\varphi V, t) = F(V, t)\, Q(V,t)$ donne $F(\varphi V, t_1) = F(V, t_1)\, Q(V, t_1)$ donc $\varpi V, \varphi \varpi V, \varphi^2 \varpi V, \dots \varphi^{n-1} \varpi V$ sont les racines de $F(V, t_1) = 0$; mais $F_1(\varpi V, t) = F(V,t)\, P(V,t)$; donc changeant V en φV, &c. ces racines sont encore $\varpi V, \varpi \varphi V, \varpi \varphi^2 V, \dots \varpi \varphi^{n-1} V$ qui doivent revenir aux précédentes.

Ainsi

$\varphi \varpi$ [redacted] $V =$ [redacted] $\varpi \varphi^{b} V$,

[redacted]

$\varphi^2 \varpi V = \varphi \varpi \varphi^{b} V =$ [redacted] $\varpi \varphi^{2b} V$

$\varphi^3 \varpi V = \varphi \varpi \varphi^{2b} V = \varpi \varphi^{3b} V$, &c.

Soit $x_0 = \lambda(V)$, $x_1 = \lambda(\varphi V)$, &c. Changeant V en ϖV, x_0 se change en $\lambda(\varpi V) = x_a = \lambda(\varphi^a V)$

x_1 ———— $\lambda(\varphi \varpi V) = \lambda(\varpi \varphi^{b} V) = \lambda(\varphi^{a+b} V) = x_{a+b}$

x_2 ———— $\lambda(\varphi^2 \varpi V) = \lambda(\varpi \varphi^{2b} V) = \lambda(\varphi^{a+2b} V) = x_{a+2b}$

⋮

x_{n-1} ———————— $x_{a+(n-1)b}$.

En général x_k en x_{a+bk}, ou si l'on veut x_{ak+b} comme ci-dessus. ——— On voit qu'il y a deux marches bien distinctes à suivre.

1° Si tout ce qui précède a lieu, en se donnant deux des racines, on se donne rationnellement toutes les autres. En effet si on veut que $x_0 = \lambda(V)$ soit une Eq. $^{\text{on}}$ satisfaite, on ne peut prendre que x_k, x_{ak} et alors pour k différent de zéro, x_k change de place; donc si on se donne en outre $x_1 = \lambda(\varphi V)$ il n'y aura qu'une seule racine V qui soit possible, et $x_2, x_3, \dots$ s'exprimeront par x_0 et x_1 rationnellement.

5/ Mais la réciproque? si les racines dépendent de deux x_0, x_1, l'Éq.^{on} en V est au plus de degré $n(n-1)$, soit m son degré. Soit $x=\lambda(V)$ une des racines de $f(x)$. L'Éq.^{on} $\Pi(x-\lambda(V)) = (x-\lambda(V))(x-\lambda(V'))\ldots = 0$ n'a que des racines appartenant à $f(x)$; donc $\Pi(x-\lambda(V)) = f(x)^\mu$, et $m = n\mu$, μ est $\leq n-1$. Mais on voit que m garde le facteur n. — Il y aura μ facteurs $x-\lambda(V)$ pour lesquels $x_0 = \lambda(V)$, μ pour x_1, x_2, &c. Et de même si on avait pris $\lambda_1(V)$ qui exprime x_1 au lieu de $\lambda(V)$, &c. Et les racines qui donnent $x_0 = \lambda(V) = \lambda(V_1) = \ldots$ sont (à la première près) différentes de celles qui donnent $x_1 = \lambda_1(V) = \lambda_1(V') = \ldots$ car si $V' = V_1$ le changement de V en V_1 ou $V' = V_1$ laisserait deux racines à la même place, toutes par conséquent et on aurait $V = \text{fonct}(x_0, x_1) = V_1$ ce qui est absurde.

Ainsi $(\mu-1)$ racines pour lesquelles x_0 ne change pas, puis $(\mu-1)$ pour lesquelles x_1 ne change pas, &c, en mettant ces racines à la place de V. De là $n(\mu-1)+1$ permutations où une des racines garde sa place. Mais cela n'épuise pas les $n\mu$ racines toutes $n\mu$ permutations du groupe. Il y a donc des permutations pour lesquelles toutes les racines changent de place.

Soit φV une de ces racines, $x_0 = \lambda(V)$ devient $\lambda(\varphi V)$ que j'appelle x_1, puis $\lambda(\varphi^2 V) = x_2$, … jusqu'à $\lambda(\varphi^{s-1} V) = x_{s-1}$, $\lambda(\varphi^s V) = x_0$. Mais alors $\varphi^s V = V$, sans quoi le changement de V en $\varphi^s V$ laissant deux racines x_1, x_2 à la même place y laisse toutes les autres, et de là $\varphi^s V = f(x_0, x_1) = V$, puisque le changement de V en $\varphi^s V$ dans $V = \text{fonc. }f(x_0, x_1)$ ne change pas le second membre. D'ailleurs si $\lambda(V), \lambda(\varphi V), \ldots \lambda(\varphi^{s-1} V)$ ne représentaient pas toutes les racines x, ces n racines se partageraient en groupes d'un nombre égal de racines, ce qui est impossible, n étant premier. Ainsi $s = n$, et

$x_0 = \lambda(V)$, $x_1 = \lambda(\varphi V)$, … $x_{n-1} = \lambda(\varphi^{n-1} V)$.

Maintenant soit x_k, $x_{f(k)}$ une des permutations du groupe, on peut y appliquer la permutation tournante qui vient d'être trouvée, et aussi appliquer

6) la permutation ci-dessus par ces permutations tournantes. De là x_{k}, $x_{f(k+i)+i'}$ où i et i' ont les n valeurs $0, 1, 2, \ldots n$. De là n^2 permutations qui doivent se réduire à $n\mu$ distinctes, $\mu \leqq n-1$. Donc deux au moins sont égales et $f(k+i)+i' = f(k+i_0)+i'_0$ quel que soit k; $f(K+I) = f(K)+C$, C indép. de K et $I = i - i_0$ différent de zéro, sans quoi $i' = i'_0$ aussi, ce qui y absurdité. De là $f(I) = f(0)+C$, $f(2I) = 2f(0)+C$, $\ldots$ $f(K) = aK+b$. Ainsi nous voilà ramenés aux permutations linéaires, et l'Eq.^{on} se résout.

[illegible]

Monument de [illegible]

trouvé avec le Mémoire

d'Évariste Gallois

1)

Soit $F(V) = V^m + \&c = 0$ l'Éq. en V.

— adjoignons r racine de degré 1er $= p$. (r', r'' … autres racines n'étant pas ou pouvant ne pas être adjointes). alors $F(V)$ se décompose (si décomposition il y a) en ~~facteurs~~ tous de même degré; car avec des adjonctions données les Éq.ons auxiliaires en V ou V ne peuvent être que de même degré, leurs racines s'exprimant ~~rationnellement~~ par V et V par V. Donc

$$F(V) = f(V,r) f_1(V,r) \ldots f_{n-1}(V,r),$$

et $in = m$, i degré de de $f(V,r)$.

Mais
$$F(V) = f(V,r) f_1(V,r) \ldots$$
$$= f(V,r') f_1(V,r') \ldots$$

Donc
$$F(V)^p = \overline{f(V,r) f(V,r') \ldots f(V,r^{(p-1)})} \times \overline{f_1(V,r) f_1(V,r')} \ldots \times \ldots$$

voilà donc sans adjonctions $F(V)^p$ décomposé en facteurs de degrés égaux. Or à cause de p premiers $F(V)$. $F(V)$ .. $F(V)$ est la seule décomposition possible. Donc

$$F(V) = f(V,r) f(V,r') \ldots f(V,r^{(p-1)})$$

Ainsi à la fois

$$F(V) = f(V,r) f_1(V,r) \ldots f_{n-1}(V,r) = f(V,r) \ldots f(V,r^{(p-1)})$$

Donc $n = p$. Et le groupe est susceptible des deux décompositions répondant à

$F(V) = f(V,r) f_1(V,r) \ldots$ et à $F(V) = f(V,r) f(V,r') \ldots$

2)

Considérons les groupes qui proviennent de la décomposition

$$F(V)=f(V,r)f(V,r')\dots f(V,r^{(m-1)})$$

$f(V,r)=0$, V, φV, ψV, … indép. de r.

$f(\varphi V, r) = f(V,r)\,Q(V,r)$.

donc

$$f(\varphi V, r') = f(V,r')\,Q(V,r').$$

Donc si $V' = \varpi(V)$ est racine de $f(V',r')=0$, φV, ψV … seront les autres.

Donc des permutations du groupe

$$(V),\ (\varphi V),\ (\psi V), \dots$$

on passe à celles du groupe

$$(V'),\ (\varphi V'),\ (\psi V'), \dots$$

par le simple changement de V en V' effectué partout c'est à dire à l'aide d'une ~~[illegible]~~ même substitution opérée à la fois dans toutes les permutations du 1er groupe.

changé en λ_k.

3)

On passe du 1er groupe au 2ème par une seule substitution opérée dans les permutations du 1er.

1er groupe | $x_0 = \lambda(V),\ x_1 = \lambda_1(V), \ldots$

$\qquad\qquad x_0 = \lambda_k(\varphi V) \ldots$

Changeons V en V' pour passer au second groupe et soit $\lambda(V') = \lambda(\varpi V) = \lambda_s(V) = x_s, \ldots$ ou x_0 changé en x_s dans la première ligne. On a $x_0 = \lambda(V) = \lambda_k(\varphi V)$; donc $\lambda(V') = \lambda_k(\varphi V')$; donc dans la seconde ligne $x_0 = \lambda_k(\varphi V)$ se change aussi en x_s. Donc &c.

Considérons en second lieu les groupes qui proviennent de la décomposition

$$F(V) = f(V,r) f_1(V,r) \ldots f_{m-1}(V,r).$$

et montrons que les substitutions sont les mêmes dans chaque groupe.

$f(V,r)$ 1er groupe | $x_0 = \lambda(V),\ x_1 = \lambda_1(V), \ldots$

$\qquad\qquad x_k = \lambda(\varphi V), \ldots\ldots$

soit $f_1(\varpi V, r) = f(V,r)\,Q(V,r)$. on passe au second groupe en remplaçant V par ϖV. ~~soit~~ $x_0 = \lambda_s(\varpi V)$, au dessous de x_0 dans le second groupe sera $\lambda_s(\varpi\varphi V)$; or $\lambda(\varphi V) = \lambda_k(V)$, $\lambda(V) = \lambda_s(\varpi V)$, de la dernière on tire $\lambda(\varphi V) = \lambda_s(\varpi\varphi V) = \lambda_k(V)$; donc $\lambda_s(\varpi\varphi V) = x_k$ et au dessous de x_0 se trouve x_k dans le second comme dans le 1er groupe.

281

4). Ainsi on ~~peut~~ décomposer le groupe primitif de deux manières en groupes partiels. 1°. En groupes dont chacun se déduit d'un autre à l'aide d'une seule substitution opérée dans les permutations. 2°. En groupes qui renferment tous les mêmes substitutions.

Mais si r est $\sqrt[p]{a}$ ou si les racines r, r'.. dépendent rationnellement l'une de l'autre, les deux genres de décomposition ne peuvent manquer de coïncider. &c.

Mais soit à présent p un nombre composé.

$$F(V)^p = \overline{f(V,r)f(V,r')\dots} \cdot \overline{f_1(V,r)\dots} \quad \dots\dots \overline{f_{n-1}(V,r)\dots}$$

alors $f(V,r)f(V,r')\dots$ est de degré ip et peut être une puissance q de $F(V)$.

$$f(V,r)f(V,r')\dots f(V,r^{(p-1)}) = F(V)^q = V^{mq} + \&c.$$

donc $ip = mq$, et déjà $m = in$; donc $ip = inq$, $p = nq$.

Dans ce cas on a à la fois

$$F(V) = f(V,r)\,f_1(V,r)\dots f_{n-1}(V,r)$$

et

$$F(V)^q = f(V,r)f(V,r')\dots f(V,r^{(p-1)})$$

Il y aura donc q racines égales à V, &c. au produit

$$f(V,r)\,f(V,r')\dots f(V,r^{(p-1)})$$

Mais chaque facteur $f(V,r)$ ne peut avoir que des racines inégales. Voilà ce qu'on voit d'abord, mais approfondissons la chose.

5/. Soient $V, \varphi V, \psi V, ..$ les racines de $f(V, r)=0$. Soit ϖV une racine V' de $f(V', r')=0$. On a donc $f(\varpi V, r')=0$ et ϖV est absolument rationnelle. Mais

$$f(\varphi V, r) = f(V, r)\, Q(V, r).$$

Donc

~~[illegible]~~

$$f(\varphi V, r') = f(V, r')\, Q(V, r')$$

équation identique en V de sorte que

$$f(\varphi V', r') = f(V', r')\, Q(V', r').$$

Donc si $f(V', r')=0$, $f(\varphi V', r')$ = aussi zéro. De là les racines $V', \varphi V' \ldots$ inégales, car si $\varphi V' = \psi V'$ comme les fonctions φ, ψ (?) sont absolument rationnelles, $\varphi V = \psi V$ contre l'hypothèse.

Donc $f(V, r)$ et $f(V, r')$ ne peuvent avoir une racine commune sans être identiques. Il y aura donc q facteurs égaux à $f(V, r)$, q autres différents (?) de ceux-là et égaux à $f(V, r_1)$ ...... jusqu'à $f(V, r_n)$ et par suite

$$F(V) = f(V, r)\, f(V, r_1) \ldots f(V, r_n)$$

où $r, r_1, .. r_n$ sont $\underline{n}$ racines de l'Eq. ou irréductible de degré $p = nq$. — Ainsi deux décompositions

$$F(V) = f(V, r)\, f_1(V, r) \ldots f_{n-1}(V, r)$$

et $F(V) = f(V, r)\, f(V, r_1) \ldots\ldots f(V, r_n)$

en $\underline{n}$ groupes. — La discussion de ces deux décompositions (?) ressemble à celle-ci dessus.

6) Ainsi quand il y a décomposition du groupe, ce groupe se divise en $\underline{n}$ autres appartenant soit à $\underline{n}$ facteurs relatifs à une racine $\underline{r}$ adjointe, soit à $\underline{n}$ racines $r, r_1, \ldots r_n$. Et les autres racines $r', r'', \ldots$ ne feraient que reproduire ces $\underline{n}$ groupes si on voulait les employer.

Dans la [redacted] dernière décomposition, considérer deux des groupes partiels et vous passerez du 1er au second en opérant dans [redacted] toutes les permutations du 1er une seule substitution.

Dans la première décomposition considérer [redacted] seulement les divers groupes partiels et vous verrez que tous contiennent les mêmes substitutions.

Si les deux décompositions [redacted] coïncident la décomposition est dite propre et les groupes partiels jouissent à la fois des deux propriétés indiquées.

---

adjoindre toutes les racines peut se ramener à adjoindre une racine d'une Éq.on irréductible dont les racines s'expriment rationnellement l'une par l'autre. Donc elles dépendent alors rationnellement. Et alors les décompositions doivent coïncider.

7) Soit t racine d'une Éq.^{on} irréductible dont $r, r', \ldots$ dépendent rationnellement, et $t', t'', \ldots$ autres racines aussi. Adjoignons t. De là

$$F(V) = f(V,t)\, f_1(V,t) \ldots f_{s}(V,t)$$

$$\text{et} \quad = f(V,t)\, f(V,t'_2) \ldots f(V,t_{s-1}).$$

Or si $f(V,t)$ est le plus petit facteur rationnel possible, comme adjoindre t est aussi adjoindre $t', t'', \ldots$ voilà deux décompositions rationnelles en t en facteurs premiers. Donc l'égalité doit avoir lieu facteur par facteur et les deux décompositions coïncider. Donc &c.

Il est donc bien vrai qu'il y a une grande différence entre adjoindre une seule racine d'une Équation irréductible ou les adjoindre toutes.

285

Nouvelles notes sur la décomposition du groupe total en groupes partiels.