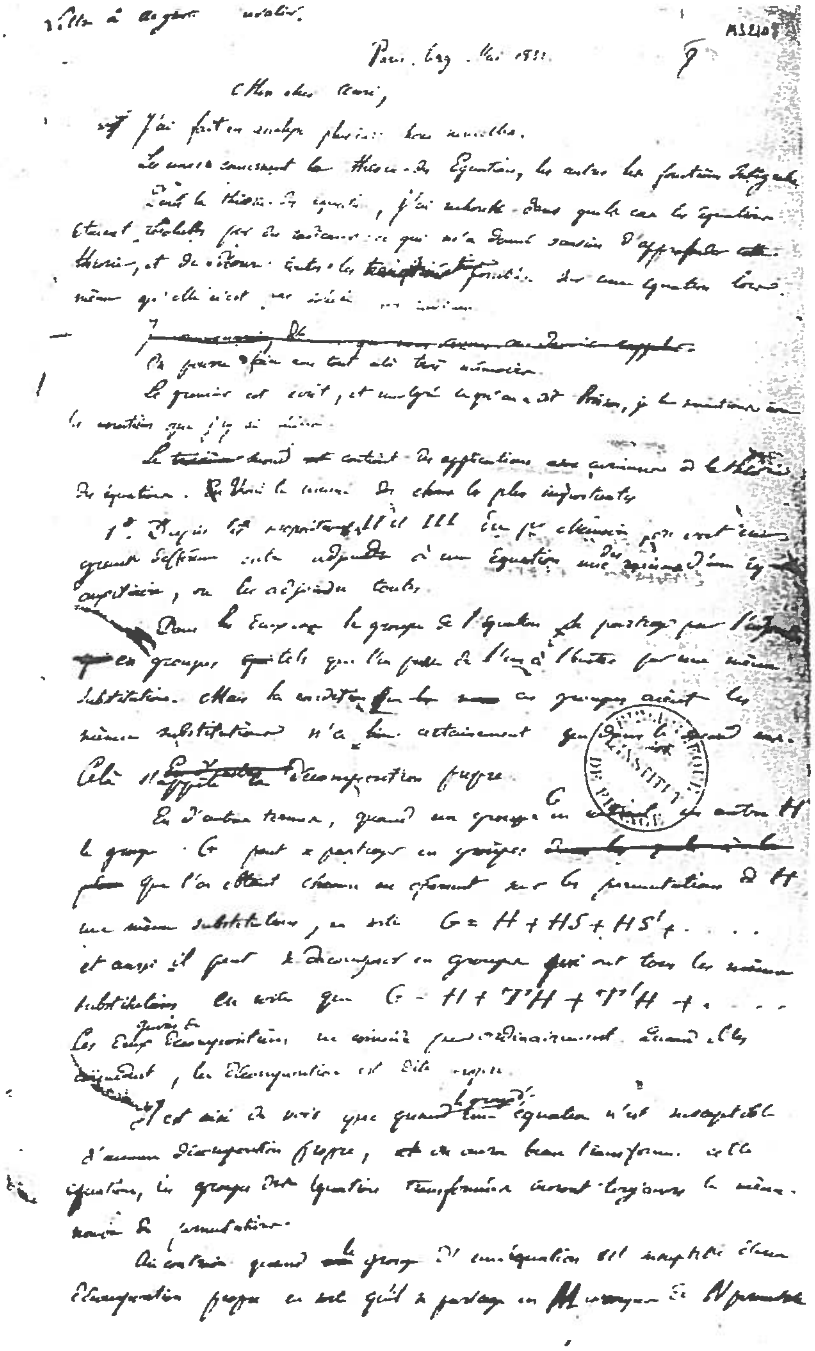
Evariste Galois
25.10.1811--31.05.1832

(A family sketch of Galois when he was 15 years old.)

GALOIS' TESTAMENTARY LETTER OF 29 MAY 1832
(written the night before the duel when he was mortally wounded.)



Lettre à Auguste Chevalier.

Paris, le 29 Mai 1832.

Mon cher Ami,

J'ai fait en analyse plusieurs choses nouvelles.

Les unes concernent la théorie des Équations, les autres les fonctions Intégrales.

Dans la théorie des équations, j'ai recherché dans quels cas les équations étaient résolubles par des radicaux, ce qui m'a donné occasion d'approfondir cette théorie, et de décrire toutes les transformations possibles sur une équation lors même qu'elle n'est pas soluble par radicaux.

On pourra faire avec tout cela trois mémoires.

Le premier est écrit, et malgré ce qu'en a dit Poisson, je le maintiens avec les corrections que j'y ai faites.

Le second contient des applications assez curieuses de la théorie des équations. Voici le résumé des choses les plus importantes.

1°. D'après les propositions II et III du 1er Mémoire, on voit une grande différence entre adjoindre à une équation une des racines d'une équation auxiliaire, ou les adjoindre toutes.

Dans les deux cas le groupe de l'équation se partage par l'adjonction en groupes tels que l'on passe de l'un à l'autre par une même substitution. Mais la condition que ces groupes aient les mêmes substitutions n'a lieu certainement que dans le second cas. Cela s'appelle la décomposition propre.

En d'autres termes, quand un groupe G en contient un autre H le groupe G peut se partager en groupes que l'on obtient chacun en opérant sur les permutations de H une même substitution, en sorte que $G = H + HS + HS' + \ldots$

et aussi il peut se décomposer en groupes qui ont tous les mêmes substitutions en sorte que $G = H + TH + T'H + \ldots$

Ces deux genres de décompositions ne coïncident pas ordinairement. Quand elles coïncident, la décomposition est dite propre.

Il est aisé de voir que quand le groupe d'une équation n'est susceptible d'aucune décomposition propre, on aura beau transformer cette équation, les groupes des équations transformées auront toujours le même nombre de permutations.

Au contraire quand le groupe d'une équation est susceptible d'une décomposition propre en sorte qu'il se partage en M groupes de N permutations

indiquent toutes les racines x. Ces indices sont pris suivant le module p, c'est à dire que la racine sera la même quand on ajoutera à l'un des indices un multiple de p.

Le groupe qu'on obtient en opérant toutes les substitutions de cette forme linéaire, contient en tout $p^n(p^n-1)(p^n-p)\ldots(p^n-p^{n-1})$ permutations.

Il s'en faut que dans cette généralité les équations qui lui répondent soient solubles par radicaux.

La condition que j'ai indiquée dans le bulletin Férussac pour que l'équation soit soluble par radicaux est trop restreinte. Il y a peu d'exceptions, mais il y en a.

générale

La dernière application de la théorie des équations est relative aux équations modulaires des fonctions elliptiques.

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

$$x_{k,l} \qquad x_{ak+bl,\,ck+dl}$$

Par conséquent l'équation modulaire correspondante aura pour groupe

$$x_{\frac{k}{l}} \qquad x_{\frac{ak+bl}{ck+dl}}$$

Dans laquelle $\frac{k}{l}$ peut avoir les $p+1$ valeurs ∞ 0 1 2 ... $p-1$.

Ainsi en convenant que k peut être infini, on peut écrire simplement

$$x_k \qquad x_{\frac{ak+b}{ck+d}}$$

en donnant à a b c d toutes les valeurs, on obtient $(p+1)p(p-1)$ permutations.

Or ce groupe se décompose ~~proprement~~ en deux groupes, dont les substitutions sont

$$x_k \qquad x_{\frac{ak+b}{ck+d}}$$

$ad-bc$ étant un résidu quadratique de p.

Le groupe ainsi simplifié est de $(p+1)p\frac{p-1}{2}$ permutations.

Mais il est aisé de voir qu'il n'est plus décomposable proprement
à moins que $p=2$ ou $p=3$.
Ainsi de quelque manière que l'on transforme l'équation, son groupe

On pourra voir ensuite qu'on peut toujours transformer une intégrale donnée en une autre dans laquelle la première période soit divisée par le nombre premier p, et les 2n−1 autres restent les mêmes.

Il ne reste donc à comparer que des intégrales où les périodes seront les mêmes de part et d'autre, et telles par conséquent que n termes de l'une s'expriment sans autre équation qu'une seule du degré n, au moyen de ceux de l'autre, et réciproquement. Ici nous ne savons rien.

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

Tu feras imprimer cette lettre dans la Revue encyclopédique.

Je me suis souvent hasardé dans ma vie à avancer des propositions dont je n'étais pas sûr. Mais tout ce que j'ai écrit là est depuis bientôt un an dans ma tête, et il est trop de mon intérêt de ne pas me tromper pour qu'on me soupçonne d'avoir énoncé des théorèmes dont je n'aurais pas la démonstration complète.

Tu prieras publiquement Jacobi ou Gauss de donner leur avis non sur la vérité, mais sur l'importance des théorèmes.

Après cela il y aura, j'espère, des gens qui trouveront leur profit à déchiffrer tout ce gâchis.

Je t'embrasse avec effusion. E. Galois. Le 29 Mai 1832.

Letter to Auguste Chevalier.

Paris, 29 May 1832

My dear friend,

I have done several new things in analysis.

Some concern the theory of equations, others integral functions.

In the theory of equations I have looked for the circumstances under which equations were soluble by radicals; this has given me occasion to deepen this theory and to describe all possible transformations on an equation even in case it is not soluble by radicals.

~~I will begin, &c. ... that we have believed we should recall.~~

Three memoirs could be made from all this.

The first is written, and in spite of what Poisson has said about it I stand by it with the corrections that I have made in it.

The ~~third~~ second ~~is~~ contains some pretty interesting applications of the theory of equations. Here is a summary of the most important things.

1° According to Propositions II and III of the first memoir one sees a great difference between adjoining to an equation one of the roots of an auxiliary equation or adjoining them all.

In both cases the group of the equation is partitioned by the adjunction into groups such that one passes from one to another by one and the same substitution; but the condition that these groups should have the same substitutions does not necessarily hold except in the second case. ~~In other w[ords]~~ That is called a proper decomposition.

In other words, when a group G contains another H, the group G can be partitioned into groups ~~in which in the place~~ each of which is obtained by operating on the permutations of H with one and the same substitution, so that $G = H + HS + HS' + \cdots$. And also it can be decomposed into groups all of which have the same substitutions, so that $G = H + TH + T'H + \cdots$. These two kinds of decomposition do not ordinarily coincide. When they coincide the decomposition is said to be proper.

It is easy to see that when the group of an equation is not susceptible of any proper decomposition one may transform the equation at will, and the groups of the transformed equations will always have the same number of permutations.

When, on the contrary, the group of an equation is susceptible of a proper decomposition, so that it is partitioned into M groups of N permutations,

one will be able to solve the given equation by means of two equations: the one will have a group of M permutations, the other one of N permutations.

Therefore once one has effected ~~in an equation~~ on the group of an equation all possible proper decompositions on this group, one will arrive at groups which one will be able to transform, but in which the number of permutations will always be the same.

If each of these groups has a prime number of permutations the equation will be soluble by radicals; if not, not.

The smallest number of permutations which can have an indecomposable group, when this number is not prime, is 5.4.3.

2° The simplest ~~substitutions~~ decompositions are those which arise by the method of Mr Gauss.

~~Whenever, on adjunction of one of the roots of an equation, the equation becomes red[ucible]~~

Since these decompositions are obvious, even in the actual form of the equation, it is useless to pause for long on this topic.

What decompositions are practicable on an equation which is not ~~reducible~~ simplifiable by the method of Mr Gauss?

I have called those equations which ~~enjoy~~ cannot be simplified by the method of Mr Gauss primitive; not that these equations will really be indecomposable because they could even be soluble by radicals.

As a lemma for the theory of primitive equations that are soluble by radicals, I ~~placed~~ published in June 1830 in Férussac's *Bulletin* an analysis of imaginaries in the theory of numbers.

The proof of the following theorems is attached:

1. In order that a primitive equation shall be soluble by radicals it must be of degree p^ν, p being prime.

2. ~~Such an~~ All the permutations of such an equation will be of the form

$$x_{k,l,m,\ldots} \quad / \quad x_{ak+bl+cm+\cdots+f,\, a_1k+b_1l+c_1m+\cdots+g,\ldots}$$

$k, l, m, \ldots$ being ν indices, which, taking p values each,

indicate all the roots. The indices are taken modulo p; that is to say the root will be the same when a multiple of p is added to any one of the indices.

The group that is obtained by operating with all the substitutions of this linear form contains in all $p^\nu(p^\nu-1)(p^\nu-p)\cdots(p^\nu-p^{\nu-1})$ permutations.

It is not the case that in this generality the corresponding equations are soluble by radicals.

The condition that I indicated in Férussac's *Bulletin* in order that the equation should be soluble by radicals is too restrictive; there are few exceptions, but there are some.

~~I do not have~~

The last application of the theory of equations relates to the modular equations of elliptic functions.

It is known that the group of the equation which has for its roots the sines of the amplitudes of the $p^2 - 1$ divisions of a period is this:

$$x_{k,l} \qquad x_{ak+bl,\, ck+dl} \,.$$

Consequently the corresponding modular equation will have for group

$$x_{\frac{k}{l}} \qquad x_{\frac{ak+bl}{ck+dl}} \,,$$

in which $\frac{k}{l}$ can take the $p+1$ values ∞, 0, 1, 2, ..., $p-1$. Thus, with the convention that k may be infinite one can simply write

$$x_k \qquad x_{\frac{ak+b}{ck+d}} \,.$$

Giving to a, b, c, d all the values one obtains $(p+1)p(p-1)$ permutations.

Now this group may be *properly* decomposed into two groups, whose substitutions are

$$x_k \qquad x_{\frac{ak+b}{ck+d}} \,,$$

$ad - bc$ being a quadratic residue of p.

Thus simplified the group has $(p+1)p.\frac{p-1}{2}$ permutations. But it is easy to see that it is not further decomposable properly unless $p = 2$ or $p = 3$.

Thus in whatever way one transforms the equation its group will

always have the same number of permutations.

But it is interesting to know if the degree can be reduced.

And to begin with, it cannot be reduced below p, because an equation of degree smaller than p cannot have p as a factor in the number of permutations of its group.

Let us see then whether the equation of degree $p+1$ whose roots x_k are ~~obtained~~ indicated by giving to k all its values, including infinity, and of which the group has for substitutions

$$x_k \qquad x_{\frac{ak+b}{ck+d}},$$

$ad - bc$ being a square, may be reduced to degree p.

Well, for that it is necessary that the group may be decomposed (improperly of course) into p groups each of $(p+1)\dfrac{p-1}{2}$ permutations.

Let 0 and ∞ be two letters that are linked in one of these groups. The substitutions which do not make 0 and ∞ change their places will be of the form

$$x_k \qquad x_{m^2 k}.$$

Therefore if ~~K is neither zero nor infinity~~ M is the letter linked with 1 the letter linked with m^2 will be $m^2 M$. When M is a square one will therefore have $M^2 = 1$. But this simplification cannot take place except for $p = 5$.

~~In the 7th~~ For $p = 7$ one finds a group of $(p+1)\dfrac{p-1}{2}$ permutations, in which ∞, 1, 2, 4 have respectively 0, 3, 6, 5 for linked letters.

This group has its substitutions of the form

$$x_k \qquad x_{a\frac{k-b}{k-c}},$$

b being the letter linked with c, and a a letter [coefficient] which is ~~simultaneously~~ residue or non-residue at the same time as $b - c$.

For $p = 11$ the same substitutions will occur with the same notation,

	∞	1	3	4	5	9 having respectively
for their linked letters	0	2	6	8	10	7

~~In all~~ Thus for the cases $p = 5, 7, 11$ the modular equation is reducible to degree p.

In all rigour this reduction is not possible in the higher cases.

The third memoir concerns integrals.

It is known that a sum of terms of the same elliptic function always reduces to a single term plus algebraic or logarithmic quantities.

There are no other functions for which this property holds.

But absolutely analogous properties replace it in all integrals of algebraic functions.

~~Let~~ ~~Let us treat at the same time~~

Let us treat at one and the same time all ~~functions~~ integrals of which the differential is ~~such~~ a function of the variable and of an irrational function of the variable, whether this irrational is or is not a radical, whether or not it may be expressed by radicals.

One finds that the number of distinct periods of the most general integral relative to a given irrational is ~~2#~~ always an even number.

Letting $2n$ be this number one has the following theorem:

An arbitrary sum of terms reduces to n terms plus some algebraic and logarithmic quantities.

Functions of the first kind are those in which the algebraic and logarithmic part is null.

Of these there are n distinct ones.

The functions of the second kind are those ~~of which~~ for which the complementary part is purely algebraic.

Of these there are n distinct ones.

~~The other funct[ions]~~ One can suppose that the differentials of other functions are never infinite except once for $x = a$, and further that their complementary part reduces to a single logarithm $\log P$, P being an algebraic quantity. Denoting these functions by $\Pi(x, a)$ one will have the theorem:

$$\Pi(x,a) - \Pi(a,x) = \sum \varphi a \; \psi x \,,$$

φa and ψx being functions of the first and second kinds. It may be deduced from that ~~for the functions~~, calling $\Pi(a)$ and ψ the periods of $\Pi(x, a)$ and ψx relative to one and the same revolution of x,

$$\Pi(a) = \psi \times \varphi \, a \,.$$

Thus the periods of functions of the third kind are always expressible in terms of functions of the first and second kind.

One can also deduce from it some theorems analogous to the ~~fam[ous]~~ theorem of Legendre

$$E'F'' - E''F' = \frac{\pi}{2}\sqrt{-1}.$$

The reduction of functions of the third kind to definite integrals, which is the most beautiful discovery of Mr Jacobi, is not possible beyond the case of elliptic functions.

Multiplication of integral functions by a ~~prime?~~ whole number is always possible, like addition, by means of an equation of degree n whose roots are the values to be substituted into the integral in order to obtain the reduced terms.

The equation which gives the division of the periods into p equal parts is of degree $p^{2n} - 1$. Its group has $(p^{2n} - 1)(p^{2n} - p) \cdots (p^{2n} - p^{2n-1})$ permutations in all.

The equation which gives the division of a sum of n terms into p equal parts is of degree p^{2n}. It is soluble by radicals.

On transformation.

To begin with, following reasoning analogous to that which Abel wrote down in his last memoir, one can show that if in such a relation between integrals one has the two functions $\int \Phi(x, X)\, dx$, $\int \Psi(y, Y)\, dy$, the latter integral having $2n$ periods, ~~one may~~ it will be permissible to suppose that y and Y may be expressed as functions of x and of X by means of a single equation of degree n.

Accordingly one may suppose that the transformations always take place solely between two integrals because clearly, taking an arbitrary rational function of y and of Y, one will have

$$\sum \int f(y, Y)\, dy = \int F(x, X)\, dx + \text{an ~~alg[ebraic] and log[arithmic] quant[ity]~~}$$

There will be some obvious reductions of this equation in the case where the integrals of the one and the other member do not both have the same number of periods.

Thus we only have to compare integrals which both have the same number of periods.

It may be shown that the smallest degree of irrationality of two such integrals cannot be larger for the one than for the other.

One then shows that one can always transform a given integral into another in which ~~all the~~ one period of the former is divided by the prime number p and ~~all~~ the other $2n - 1$ remain the same.

It will then only remain to compare integrals where the periods will be the same on both sides, and consequently such that n terms of the one are expressible in terms of those of the other by means of only a single equation of degree n, and vice-versa. Here we know nothing.

You know my dear Auguste that these subjects are not the only ones that I have explored. ~~But it needed~~ For some time my main thinking was directed towards the application to transcendental analysis of the theory of ambiguity. It was concerned with seeing *a priori* in relations between transcendental quantities or functions what exchanges one could make, what quantities one could substitute for the given quantities, without the relation ceasing to hold.

That makes immediately recognisable the impossibility of many expressions that one could look for. But I do not have the time, and my ideas are not yet well enough developed in this area, which is immense.

You will have this letter printed in the *Revue Encyclopédique*.

~~In fact~~ Often in my life I have risked advancing propositions of which I was not certain. But all that I have written here has been in my head for almost a year and it is not in my interest to make a mistake so that one could suspect me of having announced theorems of which I did not have the complete proof.

You will ~~engage~~ publicly ask Jacobi ~~and~~ or Gauss to give their opinion not on the truth but on the importance of the theorems.

After that there will, I hope, be people who will find profit in deciphering all this mess.

I embrace you warmly.

E Galois 29 May 1832.